日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

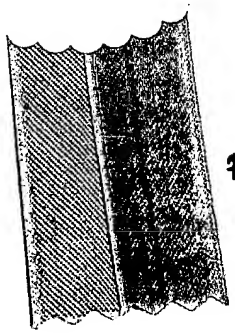
EKU

出願年月日
Date of Application: １９９９年　４月１２日

出願番号
Application Number: 平成１１年特許願第１０３９９３号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２０００年　３月１０日

特許庁長官
Commissioner,
Patent Office

近藤隆彦

出証番号　出証特２０００－３０１５８１０

【書類名】　特許願

【整理番号】　9900015709

【提出日】　平成11年 4月12日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大石　丈於

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　武藤　明宏

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項１】　暗号化されている第１の情報を保持する保持手段と、

前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を、前記第１の情報に対応させて記憶する記憶手段と、

前記保持手段により保持されている暗号化されている前記第１の情報と、前記記憶手段により記憶されている前記第２の情報を所定のプロバイダに送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項２】　暗号化されている第１の情報を保持する保持ステップと、

前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を、前記第１の情報に対応させて記憶する記憶ステップと、

前記保持ステップで保持された暗号化されている前記第１の情報と、前記記憶ステップで記憶された前記第２の情報を所定のプロバイダに送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項３】　暗号化されている第１の情報を保持する保持ステップと、

前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を、前記第１の情報に対応させて記憶する記憶ステップと、

前記保持ステップで保持された暗号化されている前記第１の情報と、前記記憶ステップで記憶された前記第２の情報を所定のプロバイダに送信する送信ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項４】　所定のプロバイダから送信されてくる、暗号化されている第１の情報、および前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を受信する受信手段と、

前記受信手段により受信された前記第２の情報に対応して、前記第１の情報の

価格条件と前記価格条件に対応する価格内容を含む第３の情報を作成する作成手段と、

前記受信手段により受信された暗号化されている前記第１の情報および前記第２の情報、並びに前記作成手段により作成された前記第３の情報を、所定の機器に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項５】　所定のプロバイダから送信されてくる、暗号化されている第１の情報、および前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、

前記受信ステップで受信された前記第２の情報に対応して、前記第１の情報の価格条件と前記価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、

前記受信ステップで受信された暗号化されている前記第１の情報および前記第２の情報、並びに前記作成ステップで作成された前記第３の情報を、所定の機器に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項６】　所定のプロバイダから送信されてくる、暗号化されている第１の情報、および前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、

前記受信ステップで受信された前記第２の情報に対応して、前記第１の情報の価格条件と前記価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、

前記受信ステップで受信された暗号化されている前記第１の情報および前記第２の情報、並びに前記作成ステップで作成された前記第３の情報を、所定の機器に送信する送信ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項７】　所定の基準情報を記憶する記憶手段と、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、前記第

１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報、および前記第１の情報の価格条件と前記価格条件に対応する価格内容を含む第３の情報を受信する受信手段と、

前記記憶手段に記憶されている前記基準情報に対応する、前記受信手段により受信された前記第２の情報の前記利用条件を選択する利用条件選択手段と、

前記記憶手段に記憶されている前記基準情報に対応する、前記受信手段により受信された前記第３の情報の前記価格条件を選択する価格条件選択手段と、

前記利用条件選択手段により選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第１の情報を復号して、利用する利用手段と、

前記価格条件選択手段により選択された前記価格条件に対応する前記価格内容に従って、前記利用手段による利用に対する課金処理を実行する実行手段と

を備えることを特徴とする情報処理装置。

【請求項８】　所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報、および前記第１の情報の価格条件と前記価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第２の情報の前記利用条件を選択する利用条件選択ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第３の情報の前記価格条件を選択する価格条件選択ステップと、

前記利用条件選択ステップで選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第１の情報を復号して、利用する利用ステップと、

前記価格条件選択ステップで選択された前記価格条件に対応する前記価格内容に従って、前記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

【請求項９】　所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、前記第１の情報の利用条件と前記利用条件に対応する利用内容を含む第２の情報、および前記第１の情報の価格条件と前記価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第２の情報の前記利用条件を選択する利用条件選択ステップと、

前記記憶ステップで記憶された前記基準情報に対応する、前記受信ステップで受信された前記第３の情報の前記価格条件を選択する価格条件選択ステップと、

前記利用条件選択ステップで選択された前記利用条件に対応する前記利用内容に従って、暗号化されている前記第１の情報を復号して、利用する利用ステップと、

前記価格条件選択ステップで選択された前記価格条件に対応する前記価格内容に従って、前記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【０００２】

【従来の技術】

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、その情報処理装置でコンテンツを復号して、利用するシステムがある。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来のシステムにおいては、ユーザの性別や年齢などの個人情

報、コンテンツの利用実績、またはユーザの所有する情報処理装置の種類に応じて、コンテンツの利用を提供するなど、変化に富んだサービスを提供することができない課題があった。

【０００４】

本発明はこのような状況に鑑みてなされたものであり、変化に富んだサービスを提供することができるようにするものである。

【０００５】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、暗号化されている第１の情報を保持する保持手段と、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶手段と、保持手段により保持されている暗号化されている第１の情報と、記憶手段により記憶されている第２の情報を所定のプロバイダに送信する送信手段とを備えることを特徴とする。

【０００６】

請求項２に記載の情報処理方法は　暗号化されている第１の情報を保持する保持ステップと、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第１の情報と、記憶ステップで記憶された第２の情報を所定のプロバイダに送信する送信ステップとを含むことを特徴とする。

【０００７】

請求項３に記載の提供媒体は、暗号化されている第１の情報を保持する保持ステップと、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第１の情報と、記憶ステップで記憶された第２の情報を所定のプロバイダに送信する送信ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００８】

請求項１に記載の情報処理装置、請求項２に記載の情報処理方法、および請求項３に記載の提供媒体においては、暗号化されている第１の情報が保持され、第

１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報が、第１の情報に対応されて記憶され、保持された暗号化されている第１の情報と、記憶された第２の情報が所定のプロバイダに送信される。

【０００９】

請求項４に記載の情報処理装置は、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信手段と、受信手段により受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成手段と、受信手段により受信された暗号化されている第１の情報および第２の情報、並びに作成手段により作成された第３の情報を、所定の機器に送信する送信手段とを備えることを特徴とする。

【００１０】

請求項５に記載の情報処理方法は、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、受信ステップで受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第１の情報および第２の情報、並びに作成ステップで作成された第３の情報を、所定の機器に送信する送信ステップとを含むことを特徴とする。

【００１１】

請求項６に記載の提供媒体は、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、受信ステップで受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第１の情報および第２の情報、並びに作成ステップで作成された第３の情報を、所定の機器に送信する送信ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１２】

請求項４に記載の情報処理装置、請求項５に記載の情報処理方法、および請求項６に記載の提供媒体においては、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報が受信され、受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報が作成され、受信された暗号化されている第１の情報および第２の情報、並びに作成された第３の情報が、所定の機器に送信される。

【００１３】

請求項７に記載の情報処理装置は、所定の基準情報を記憶する記憶手段と、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第２の情報の利用条件を選択する利用条件選択手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第３の情報の価格条件を選択する価格条件選択手段と、利用条件選択手段により選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用手段と、価格条件選択手段により選択された価格条件に対応する価格内容に従って、利用手段による利用に対する課金処理を実行する実行手段とを備えることを特徴とする。

【００１４】

請求項８に記載の情報処理方法は、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第２の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第３の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された

利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを含むことを特徴とする。

【００１５】

請求項９に記載の提供媒体は、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第２の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第３の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１６】

請求項７に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体においては、所定の基準情報が記憶され、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報が受信され、記憶されている基準情報に対応する、受信された第２の情報の利用条件が選択され、記憶されている基準情報に対応する、受信された第３の情報の価格条件が選択され、選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報が復号され、利用され、選択された価格条件に対応する価格内容に従って、利用に対する課金処理が実行される。

【００１７】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１８】

図１は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ１、コンテンツを提供するコンテンツプロバイダ２、コンテンツに対応する所定のサービスを提供するサービスプロバイダ３、およびコンテンツが利用される機器（この例の場合、レシーバ５１およびレシーバ２０１）からなるユーザホームネットワーク５から構成されている。

【００１９】

EMDシステムに登録された機器（例えば、レシーバ５１またはレシーバ２０１）に配信（提供）されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、１つのコンテンツは、１曲分の音楽データに相当する。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入し）、提供されるコンテンツを再生したり、複製して利用する。

【００２０】

EMDサービスセンタ１は、EMDシステムにおける主な情報の流れを示す図２に示すように、ユーザホームネットワーク５、および複数のコンテンツプロバイダ２（この例の場合、２式のコンテンツプロバイダ２－１，２－２（以下、コンテンツプロバイダ２－１，２－２を個々に区別する必要がない場合、単に、コンテンツプロバイダ２と記述する。他の装置についても同様である））に、コンテンツを利用するために必要な配送用鍵Ｋｄを送信する。EMDサービスセンタ１はまた、ユーザホームネットワーク５の機器から、課金情報等を受信して、料金を精算したり、コンテンツプロバイダ２からはUCPを、そしてサービスプロバイダ３か

らPTを受信する。

【００２１】

コンテンツプロバイダ２－１，２－２は、提供するコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、そのコンテンツを復号するために必要なコンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツの利用内容などを示す取扱方針（以下、UCP(Usage Control Policy)と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ３に供給する。なお、この例の場合、２式のサービスプロバイダ３－１，３－２が存在するものとする。

【００２２】

サービスプロバイダ３－１，３－２は、コンテンツプロバイダ２から供給されるUCPに対応して、１つまたは複数の価格情報（以下、PT(Price Tag)と記述する）を作成し、それを保持する。サービスプロバイダ３は、作成したPTを、コンテンツプロバイダ２から供給されたコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク４を介して、ユーザホームネットワーク５に送信する。

【００２３】

ユーザホームネットワーク５は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS(Usage Control Status)と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク５はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵Ｋｄの供給を受けるタイミングで、対応するUCPおよびPTなどとともにEMDサービスセンタ１に送信する。なお、ユーザホームネットワーク５は、UCPおよびPTをEMDサービスセンタ１に送信しないようにすることもできる。

【００２４】

この例の場合、ユーザホームネットワーク５は、図１に示すように、HDD５２に接続され、SAM６２を有するレシーバ５１、およびHDD２０２に接続され、SAM

２１２を有するレシーバ２０１から構成されている。なお、レシーバ５１およびレシーバ２０１についての詳細は後述する。

【００２５】

図３は、EMDサービスセンタ１の機能的構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信したり、利益分配の情報を供給する。

【００２６】

著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors,Composers and Publishers:日本音楽著作権協会)に送信する。

【００２７】

鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、それを、コンテンツプロバイダ管理部１２を介してコンテンツプロバイダ２に供給したり、ユーザ管理部１８等を介してユーザホームネットワーク５に供給する。

【００２８】

ユーザホームネットワーク５の、EMDシステムに正式登録された機器およびコンテンツプロバイダ２に供給される、EMDサービスセンタ１からの配送用鍵Ｋｄについて、図４乃至図７を参照して説明する。

【００２９】

図４は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成する、例えば、レシーバ５１がコンテンツの利用を開始する、１９９８年１月における、EMDサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

【００３０】

図４の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可

能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

【００３１】

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【００３２】

また、レシーバ５１がコンテンツの利用を開始するに先立ち、EMDサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３月分の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、EMDサービスセンタ１に接続できないなどのトラブ

ルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

【００３３】

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３４】

１９９８年２月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

【００３５】

１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３６】

１９９８年３月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月

まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

【００３７】

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

【００３８】

１９９８年４月１日における、EMDサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図７で説明する。EMDサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。EMDサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

【００３９】

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、EMDサービスセンタ１、コンテンツプロバイダ２、ユーザホ

ームネットワーク５を構成するレシーバ５１で利用される。

【００４０】

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザが１，２ヶ月まったくEMDサービスセンタ１にアクセスしなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ１にアクセスして鍵を受信することができる。

【００４１】

また、ユーザホームネットワーク５の、EMDシステムに正式登録された機器、およびコンテンツプロバイダ２には、以上のように、３ヶ月分の配送用鍵Ｋｄが配布されるが、EMDシステムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク５の機器には、３ヶ月分の配送用鍵Ｋｄに代わり、図８に示すような、１ヶ月分の配送用鍵Ｋｄが配布される。この例においては、ユーザホームネットワーク５の機器をEMDシステムに正式登録するために、与信処理など、約１月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約１ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、１ヶ月間において利用可能な配送用鍵Ｋｄが配布される。

【００４２】

図３に戻り、経歴データ管理部１５は、ユーザ管理部１８から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

【００４３】

利益分配部１６は、経歴データ管理部１５から供給された各種情報に基づき、EMDサービスセンタ１、コンテンツプロバイダ２－１，２－２、およびサービスプロバイダ３－１，３－２の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に出力する。利益配分部１６はまた、算出した利益に応じてコンテンツプロバイダ２－１，２－２およびサービスプロバイダ３－１，３－２のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利

用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部１８に出力する。なお、以下において、コンテンツプロバイダ２における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ３における利用ポイントをサービス利用ポイントと称する。

【００４４】

相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の機器と相互認証を実行する。

【００４５】

ユーザ管理部１８は、EMDシステムに登録可能な、ユーザホームネットワーク５の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図９に示すように、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に設定される情報が含まれる。

【００４６】

「SAMのID」には、製造された、ユーザホームネットワーク５の機器のSAMのIDが記憶される。図９のシステム登録情報の「SAMのID」には、レシーバ５１のSAM６２のIDおよびレシーバ２０１のSAM２１２のIDが設定されている。

【００４７】

「機器番号」には、SAMを有するユーザホームネットワーク５の機器に、予め設定された機器番号が設定される。ユーザホームネットワーク５の機器が、ネットワーク４を介してサービスプロバイダ３と、およびEMDサービスセンタ１と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、このような機能を有する機器を主機器と称する）には、１００番以上の機器番号が与えられる。機器が、そのような機能を有しいない場合、その機器（以下、このような機器を従機器と称する）には、９９番以下の機器番号が与えられる。この例の場合、レシーバ５１およびレシーバ２０１の両者は、上述した機能を有しているので、それぞれには、１００番以上の機器番号（１００番）が与

えられてる。そこで、図９のシステム登録情報の「機器番号」には、レシーバ５１のSAM６２のIDおよびレシーバ２０１のSAM２１２のIDに対応する「機器番号」のそれぞれには、機器番号１００番が設定されている。

【００４８】

「決済ID」には、EMDシステムに正式登録されたとき割り当てられる所定のIDが記憶される。この例の場合、レシーバ５１は、ユーザＦが決済ユーザ（後述）として、そしてレシーバ２０１は、ユーザＡを決済ユーザとして、それぞれ正式登録され、決済IDが与えられているので、図９のシステム登録情報の、SAM６２のIDおよびSAM２１２のIDに対応する「決済ID」には、与えられた決済IDが設定されている。

【００４９】

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。

【００５０】

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザ一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザ一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに仮登録されるときに割り当てられ、設定される。

【００５１】

この例の場合、レシーバ５１は、ユーザＦが決済ユーザとして登録されている

ので、図９のシステム登録情報の、SAM６２のIDに対応する「決済ユーザ情報」には、ユーザＦから提供されたユーザ一般情報、ユーザＦのID、およびユーザＦのパスワードが設定されている。レシーバ２０１は、ユーザＡが決済ユーザとして登録されているので、SAM２１２のIDに対応する「決済ユーザ情報」には、ユーザＡから提供されたユーザ一般情報、ユーザＡのID、およびユーザＡのパスワードが設定されている。なお、この例の場合、ユーザＦは、男性で、ユーザＡは、女性とする。

【００５２】

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

【００５３】

この例の場合、レシーバ５１およびレシーバ２０１の両者には、従属ユーザが登録されていないので、図９のシステム登録情報のSAM６２のIDに対応する「従属ユーザ情報」、およびSAM２１２のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

【００５４】

「利用ポイント情報」には、利益分配部１６から出力された利用ポイントが設定される。図１０（Ａ）は、SAM６２に対応する「利用ポイント情報」に記憶されているレシーバ５１の利用ポイント情報を示している。これによれば、レシーバ５１のユーザＦ（決済ユーザ）には、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイント、コンテンツプロバイダ２－２のコンテンツ利

用ポイントが１２３ポイント、サービスプロバイダ３－１のサービス利用ポイントが３４５ポイント、そしてサービスプロバイダ３－２のサービス利用ポイントが０ポイントだけ与えられている。

【００５５】

図１０（Ｂ）は、SAM２１２に対応する「利用ポイント情報」に記憶されているレシーバ２０１の利用ポイント情報を示している。これによれば、レシーバ２０１のユーザＡ（決済ユーザ）には、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２３ポイント、コンテンツプロバイダ２－２のコンテンツ利用ポイントが２２ポイント、サービスプロバイダ３－１のサービス利用ポイントが４０ポイント、そしてサービスプロバイダ３－２のサービス利用ポイントが５ポイントだけ与えられている。

【００５６】

なお、この例において、コンテンツプロバイダ２－１およびコンテンツプロバイダ２－２のそれぞれのコンテンツ利用ポイントの合計ポイント（ユーザＦの場合は３４５（＝１２３＋２２２）、ユーザＡの場合は４５ポイント（＝２３＋２２））と、サービスプロバイダ３－１およびサービスプロバイダ３－２のそれぞれのサービス利用ポイントの合計ポイント（ユーザＦの場合は３４５（＝３４５＋０、ユーザＡの場合は４５ポイント（＝５＋４０））が等しくなるようになされている。

【００５７】

ユーザ管理部１８は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Ｋｄとともにユーザホームネットワーク５に送信する。

【００５８】

図３に、再度戻り、課金請求部１９は、経歴データ管理部１５から供給された、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部２０はまた、決算処理の結

果をユーザ管理部１８に通知する。

【００５９】

監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMDサービスセンタ１は、コンテンツプロバイダ２からのUCPを、サービスプロバイダ３からのPTを、そしてユーザホームネットワーク５からのUCPとPTを、それぞれ受け取る。

【００６０】

図１１は、コンテンツプロバイダ２－１の機能的構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマーク（電子透かし）を付加し、圧縮部３３に供給する。

【００６１】

圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ATRAC2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００６２】

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをEMDサービスセンタ１から供給された配送用鍵Ｋｄを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

【００６３】

DESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する

部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【００６４】

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

【００６５】

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００６６】

ポリシー記憶部３７は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部３８に出力する。図１２は、コンテンツサーバ３１に保持されているコンテンツＡに対応して設定され、ポリシー記憶部３７に記憶されているUCPA、Ｂを表している。UCPには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、「利用内容」の各項目に設定される情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPA（図１２（Ａ））およびUCPＢ（図１２（Ｂ））のそれぞれの「コンテンツのID」には、コンテンツＡのIDが設定されている。

【００６７】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPＡおよびUCPＢのそれぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ２－１のIDが設定されている。「UCPのID」

には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

【００６８】

「利用条件」は、「ユーザ条件」および「機器条件」の項目からなり、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定される。

【００６９】

UCPAの場合、「利用条件１０」が設定され、「利用条件１０」の「ユーザ条件１０」には、利用ポイントが２００ポイント以上であることが条件であることを示す情報（”２００ポイント以上”）が設定されている。また「利用条件１０」の「機器条件１０」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、UCPAは、２００ポイント以上のコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【００７０】

UCPBの場合、「利用条件２０」が設定され、「利用条件２０」の「ユーザ条件２０」には、利用ポイントが２００ポイントより少ないことが条件であることをを示す情報（”２００ポイントより少ない”）が設定されている。また「利用条件２０」の「機器条件２０」には、”条件なし”が設定されている。すなわち、UCPBは、２００ポイントより少ないコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

【００７１】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」などの項目からなり、その「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【００７２】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定されている。コンテンツの管理移動が行われると、図１３（Ａ）に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図１３（Ｂ）に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

【００７３】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図１３（Ａ）に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の２機においてのみコンテンツが保持される。この点で、図１４（Ａ）に示すように、オリジナルのコンテンツから、複数の複製（第１世代）を作成することができる、第１世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図１４（Ｂ）に示すように、１回だけの複製とも異なる。

【００７４】

図１２（Ａ）に戻り、UCPAには、４つの「利用内容１１」乃至「利用内容１４」が設けられており、「利用内容１１」において、その「ID１１」には、「利用内容１１」に割り当てられた所定のIDが設定されている。「形式１１」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ１１」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報１１」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

【００７５】

「利用内容１２」において、その「ID１２」には、「利用内容１２」に割り当てられた所定のIDが設定されている。「形式１２」には、第１世代の複製を行う

利用形式を示す情報（”第１世代複製”）が設定されている。第１世代複製は、図１４（Ａ）に示したように、オリジナルのコンテンツから、複数の第１世代の複製を作成することができる。ただし、第１世代の複製から第２世代の複製を作成することはできない（許可されない）。「パラメータ１２」には、”第１世代複製”に対応する所定の情報が設定されている。「管理移動許可情報１２」には、コンテンツの管理移動が許可されていないことを示す”不可”が設定されている。

【００７６】

「利用内容１３」において、その「ID１３」には、「利用内容１３」に割り当てられた所定のIDが設定されている。「形式１３」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ１３」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報１３」には、”不可”が設定されている。

【００７７】

「利用内容１４」において、その「ID１４」には、「利用内容１４」に割り当てられた所定のIDが設定されている。「形式１４」には、５回の複製を行う利用形式（いわゆる、５回複製することができる回数券）を示す情報（”Pay Per Copy５”）が設定されている。なお、この場合も、図１４の（Ｂ）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ１４」には、”Pay Per Copy５”に対応して、複製が５回可能であることを示す情報”複製５回”が設定されている。「管理移動許可情報１４」には、”不可”が設定されている。

【００７８】

図１２（Ｂ）のUCPＢには、２つの「利用内容２１」および「利用内容２２」が設けられている。「利用内容２１」において、その「ID２１」には、「利用内容２１」に割り当てられた所定のIDが設定されている。「形式２１」には、４回の再生を行う利用形式を示す情報（”Pay Per Play４”）が設定され、「パラメータ２１」には、再生が４回可能であることを示す情報（”再生４回”）が設定

されている。「管理移動許可情報２１」には、”不可”が設定されている。

【００７９】

「利用内容２２」において、その「ID２２」には、「利用内容２２」に割り当てられた所定のIDが設定されている。「形式２２」には、”Pay Per Copy２”が設定され、「パラメータ２２」には、”複製２回”が設定されている。「管理移動許可情報２２」には、”不可”が設定されている。

【００８０】

ここで、UCPAおよびUCPBの内容を比較すると、２００ポイント以上の利用ポイントを有するユーザは、４通りの利用内容１１乃至利用内容１４から利用内容を選択することができるのに対して、２００ポイントより少ない利用ポイントを有するユーザは、２通りの利用内容２１，２２からしか利用内容を選択することができないものとされている。

【００８１】

ところで、図１２は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件１０」およびUCPBの「利用条件２０」は、図１５（A）に示すサービスコード、および図１５（B）に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードにより、実際は構成されている。

【００８２】

図１６（A）は、UCPA（図１２（A））の「利用条件１０」の「ユーザ条件１０」および「機器条件１０」として設定されている各コードのコード値を表している。UCPAの「利用条件１０」の「ユーザ条件１０」は、”２００ポイント以上”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコード（図１５（A））が、このとき数値２００を示す０００Ｃ８ｈのバリューコードが、そして”＞＝（以上）”を意味する０６ｈのコンディションコード（図１５（B））が、ユーザ条件として設定されている。

【００８３】

UCPAの「機器条件１０」は、”条件なし”とされているので、”条件なし”を意味する０００００ｈのサービスコードが、このとき何ら意味を持たないＦＦＦ

ＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが、機器条件として設定されている。

【００８４】

図１６（Ｂ）は、UCPBの「利用条件２０」の「ユーザ条件２０」および「機器条件２０」として設定されている各コードのコード値を表している。「ユーザ条件２０」は、”２００ポイントより少ない”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコードが、数値２００を示す００００Ｃ８ｈのバリューコードが、そして”＜（より小さい）”を意味する０３ｈのコンディションコードが、ユーザ条件として設定されている。

【００８５】

UCPBの「機器条件２０」は、UCPAの「機器条件１０」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

【００８６】

図１１に戻り、セキュアコンテナ作成部３８は、例えば、図１７に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびUCPA，Ｂの全体）にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ２－１の秘密鍵Ｋｓｃｐ）で暗号化されたものである。

【００８７】

セキュアコンテナ作成部３８はまた、コンテンツプロバイダセキュアコンテナに、図１８に示すコンテンツプロバイダ２－１の証明書を付してサービスプロバイダ３に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２－１に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ２－１の名前、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐ、並びに

その署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）から構成されている。

【００８８】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【００８９】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【００９０】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1などが用いられる。

【００９１】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【００９２】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるpおよびqを求め、さらにpとqの積で

あるｎを求める。(p-1)と(q-1)の最小公倍数Lを算出し、更に、３以上L未満で、かつ、Ｌと互いに素な数eを求める（すなわち、eとLを共通に割り切れる数は、１のみである）。

【００９３】

次に、Lを法とする乗算に関するeの乗法逆元dを求める。すなわち、d, e、およびLの間には、ed=1 mod Lが成立し、dはユークリッドの互除法で算出できる。このとき、nとeが公開鍵とされ、p,q,およびdが、秘密鍵とされる。

【００９４】

暗号文Cは、平文Mから、式（１）の処理で算出される。

【００９５】

C=M^e mod n　(1)

暗号文Cは、式（２）の処理で平文Mに、復号される。

【００９６】

M=C^d mod n　（２）

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

【００９７】

M=C^d=(M^e)^d=M^(ed)=M mod n　（３）

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【００９８】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線y^2=x^3+ax+b上の、ある点をBとする。楕円曲線上の点の加算を定義し、nBは、Bをn回加算した結果を表す。同様に、減算も定義する。BとnBからnを算出することは、困難であることが証明されている。BとnBを公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式（４）

および式（５）の処理で算出される。

【００９９】

C1=M+rnB　（４）

C2=rB　（５）

暗号文C1およびC2は、式（６）の処理で平文Mに、復号される。

【０１００】

M=C1-nC2　（６）

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【０１０１】

図１１に、再び戻り、コンテンツプロバイダ２－１の相互認証部３９は、EMDサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、EMDサービスセンタ１と相互認証し、また、相互認証部３９は、サービスプロバイダ３へのコンテンツセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

【０１０２】

コンテンツプロバイダ２－２は、コンテンツプロバイダ２－１と基本的の同様の構成を有しているので、その図示および説明は省略する。

【０１０３】

次に、図１９のブロック図を参照して、サービスプロバイダ３－１の機能的構成を説明する。コンテンツサーバ４１は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、UCP、およびコンテンツプロバイダ２の署名を記憶し、セキュアコンテナ作成部４４に供給する。

【０１０４】

値付け部４２は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ２の証明書が検証され、正当であるとき、コンテンツプロバイダ２の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

【０１０５】

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部４４に供給する。図２０は、図１２（Ａ）のUCPＡに対応して作成された、２つのPTＡ－１（図２０（Ａ））およびPTＡ－２（図２０（Ｂ））を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に設定される情報が含まれる。

【０１０６】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」には、UCPに対応する各項目の情報が、それぞれ設定される。すなわち、PTＡ－１およびPTＡ－２のそれぞれの「コンテンツのID」には、コンテンツＡのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ２－１のIDが、そしてそれぞれの「UCPのID」には、UCPＡのIDが設定されている。

【０１０７】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ３のIDが設定される。PTＡ－１およびPTＡ－２の「サービスプロバイダのID」には、サービスプロバイダ３－１のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTＡ－１の「PTのID」には、PTＡ－１のIDが、PTＡ－２の「PTのID」には、PTＡ－２のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTＡ－１の「PTの有効期限」には、PTＡ－１の有効期限が、PTＡ－２の「PTの有効期限」には、PTＡ－２の

有効期限が設定されている。

【０１０８】

「価格条件」は、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、このPTを選択することができるユーザの条件が設定され、その「機器条件」には、このPTを選択することができる機器の条件が設定される。

【０１０９】

PTA－１の場合、「価格条件１０」が設定され、「価格条件１０」の「ユーザ条件１０」には、ユーザが男性であるを示す情報（”男性”）が設定され、その「機器条件１０」には、”条件なし”が設定されている。すなわち、PTA－１は、男性のユーザのみが選択可能となる。

【０１１０】

PTA－１の「価格条件１０」の「ユーザ条件１０」および「機器条件１０」も、実際は、図２１（A）に示すように、各種コードのコード値が設定されている。「価格条件１０」の「ユーザ条件１０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５（A））が、このとき男性を意味する０００００ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５（B））が設定されている。「機器条件１０」には、”条件なし”を意味する００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

【０１１１】

PTA－２の場合、「価格条件２０」が設定され、「価格条件２０」の「ユーザ条件２０」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件２０」には、”条件なし”が設定されている。すなわち、PTA－２は、女性のユーザのみが選択可能となる。

【０１１２】

PTA－２の「価格条件２０」の「ユーザ条件２０」および「機器条件２０」も、実際は、図２１（B）に示すように、各コードのコード値が設定されている。

「価格条件２０」の「ユーザ条件２０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５（Ａ））が、この場合女性を示す０００００１ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５（Ｂ））が設定されている。その「機器条件２０」には、”条件なし”を意味する００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

【０１１３】

図２０に戻り、PTの「価格内容」には、コンテンツが、対応するUCPの「利用内容」の「形式」に設定された利用形式で利用される場合の利用料金が示されている。すなわち、PTA－１の「価格内容１１」に設定された”２０００円”およびPTA－２の「価格内容２１」に設定された”１０００円”は、UCPA（図１２（Ａ））の「利用内容１１」の「形式１１」が”買い取り再生”とされているので、コンテンツＡの買い取り価格（料金）を示している。

【０１１４】

PTA－１の「価格内容１２」の”６００円”およびPTA－２の「価格内容２２」の”３００円”は、UCPAの「利用内容１２」の「形式１２」より、第１世代複製の利用形式でコンテンツＡを利用する場合の料金を示している。PTA－１の「価格内容１３」の”１００円”およびPTA－２の「価格内容２３」の”５０円”は、UCPAの「利用内容１３」の「形式１３」より、期間制限再生の利用形式でコンテンツＡを利用する場合の料金を示している。PTA－１の「価格内容１４」の”３００円”およびPTA－２の「価格内容２４」の”１５０円”は、UCPAの「利用内容１４」の「形式１４」より、５回の複製を行う利用形式でコンテンツＡを利用する場合の料金を示している。

【０１１５】

なお、この例の場合、PTA－１（男性ユーザに適用される）の価格内容と、PTA－２（女性ユーザに適用される）の価格内容を比較すると、PTA－１の価格内容に示される価格が、PTA－２の価格内容に示される価格の２倍に設定されている。例えば、UCPAの「利用内容１１」に対応するPTA－１の「価格内容１１」

が”２０００円”とされているのに対し、同様にUCPAの「利用内容１１」に対応するPTA－２の「価格内容２１」は”１０００円”とされている。同様、PTA－１の「価格内容１２」乃至「価格内容１４」に設定されている価格は、PTA－２の「価格内容２２」乃至「価格内容２４」に設定されている価格のそれぞれの２倍とされている。すなわち、女性ユーザは、男性ユーザに比べ、コンテンツＡを、半額の料金で利用することができる。

【０１１６】

図２２は、図１２（Ｂ）のUCPＢに対応して作成された、２つのPTＢ－１およびPTＢ－２を表している。図２２（Ａ）のPTＢ－１には、コンテンツＡのID、コンテンツプロバイダ２－１のID、UCPＢのID、UCPＢの有効期限、サービスプロバイダ３－１のID、PTＢ－１のID、PTＢ－１の有効期限、価格条件３０、２通りの価格内容３１，３２などが含まれている。

【０１１７】

PTＢ－１の「価格条件３０」の「ユーザ条件３０」には”条件なし”が設定され、「機器条件３０」には、機器が従機器であることを示す情報（”従機器”）が設定されている。すなわち、PTＢ－１は、コンテンツＡが従機器において利用される場合にのみ選択可能となる。

【０１１８】

PTＢ－１の「価格条件３０」の「ユーザ条件３０」および「機器条件３０」にも、実際は、図２３（Ａ）に示すように、各コードのコード値が設定されている。「ユーザ条件３０」には、”条件なし”を意味する００００ｈのサービスコード（図１５（Ａ））が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（図１５（Ｂ））が設定されている。「機器条件３０」は、”従機器”とされているので、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＜（小さい）”を意味する０３ｈのコンディションコードが設定されている。この例の場合、従機器には、１００番より小さい機器番号が設定されているので、このようなコード値が設定される。

【０１１９】

PTB－１の「価格内容３１」の”１００円”は、UCPB（図１２（B））の「利用内容２１」の「形式２１」が”Pay Per Play4”とされているので、４回の再生を行う場合の料金を示し、「価格内容３２」の”３００円”は、UCPBの「利用内容２２」の「形式２２」が”Pay Per Copy2”とされているので、２回の複製を行う場合の料金を示している。

【０１２０】

UCPBに対応して作成された、もう一方の図２２（B）のPTB－２には、コンテンツAのID、コンテンツプロバイダ２－１のID、UCPBのID、サービスプロバイダ３－１のID、PTB－２のID、PTB－２の有効期限、価格条件４０、および２通りの価格内容４１，４２などが含まれている。

【０１２１】

PTB－２の「価格条件４０」の「ユーザ条件４０」には”条件なし”が設定され、その「機器条件４０」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、PTB－２は、主機器においてコンテンツAが利用される場合にのみ選択可能となる。

【０１２２】

PTB－２の「価格条件４０」の「ユーザ条件４０」および「機器条件４０」にも、実際は、図２３（B）に示すように、各コードのコード値が設定されている。「価格条件４０」の「ユーザ条件４０」には、”条件なし”を意味する００００hのサービスコード（図１５（A））が、この場合何ら意味を持たないＦＦＦＦＦＦhのバリューコードが、そして”無条件”を意味する００hのコンディションコード（１５（B））が設定されている。「機器条件４０」には、”機器に関し条件有り”を意味する００ｘｘhのサービスコードが、このとき”数値１００”を示す０００００６４hのバリューコードが、そして”＝＞（以上）”を意味する０６hのコンディションコードが設定されている。

【０１２３】

PTB－２の「価格内容４１」および「価格内容４２」のそれぞれに示される価格は、UCPBの「利用内容２１」の「形式２１」および「利用内容２２」の「形

式２２」のそれぞれに示される利用形式でコンテンツＡを利用する場合の料金を示している。

【０１２４】

ここで、PTB－１（従機器に適用される）の価格内容とPTB－２（主機器に適用される）の価格内容を比較すると、PTB－１の価格内容は、PTB－２の価格内容の２倍に設定されている。例えば、PTB－１の「価格内容３１」が”１００円”とされているのに対し、PTB－２の「価格内容４１」は５０円とされており、「価格内容３２」が”３００円”とされているのに対して、「価格内容４２」は”１５０円”とされている。

【０１２５】

図１９に戻り、ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツのUCPを記憶し、セキュアコンテナ作成部４４に供給する。

【０１２６】

セキュアコンテナ作成部４４は、例えば、図２４に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ、コンテンツプロバイダ２の署名、PTＡ－１，Ａ－２，Ｂ－１，Ｂ－２、およびサービスプロバイダ３の署名からなるサービスプロバイダセキュアコンテナを作成する。

【０１２７】

セキュアコンテナ作成部４４はまた、作成したサービスプロバイダセキュアコンテナを、図２５に示すような、証明書のバージョン番号、認証局がサービスプロバイダ３－１に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３－１の名前、サービスプロバイダ３－１の公開鍵Ｋｐｓｐ、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク５に供給する。

【０１２８】

図１９に、再び戻り、相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロ

バイダ２と相互認証する。相互認証部４５また、ユーザホームネットワーク５へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証するが、このサービスプロバイダ３とユーザホームネットワーク５との相互認証は、例えば、ネットワーク４が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ３は、コンテンツプロバイダ２およびユーザホームネットワーク５と相互認証を行わなくてもよい。

【０１２９】

サービスプロバイダ３－２の構成は、サービスプロバイダ３－１の構成と基本的に同様であるので、その図示および説明は省略する。

【０１３０】

次に、図２６のブロック図を参照して、ユーザホームネットワーク５を構成するレシーバ５１の構成例を説明する。レシーバ５１は、通信部６１、SAM６２、外部記憶部６３、伸張部６４、通信部６５、インタフェース６６、表示制御部６７、および入力制御部６８より構成されている。通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはEMDサービスセンタ１と通信し、所定の情報を受信し、または送信する。

【０１３１】

SAM６２は、相互認証モジュール７１、課金処理モジュール７２、記憶モジュール７３、復号／暗号化モジュール７４、およびデータ検査モジュール７５からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

【０１３２】

SAM６２の相互認証モジュール７１は、記憶モジュール７３に記憶されている、図２７に示すSAM６２の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ｋｔｅｍｐ（セッション

鍵）を復号／暗号化モジュール７４に供給する。SAMの証明書には、コンテンツプロバイダ２－１の証明書（図１８）およびサービスプロバイダ３－１の証明書（図２５）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

【０１３３】

課金処理モジュール７２は、選択されたUCPの利用内容に基づいて、UCSおよび課金情報を作成する。図２８は、図１２（Ａ）に示したUCPＡの利用内容１１と、図２０（Ａ）に示したPTＡ－１に基づいて作成されたUCSＡを表している。UCSには、図２８に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」などの項目に設定される情報が含まれている。

【０１３４】

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図２８のUCSＡの、「コンテンツのID」には、コンテンツＡのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ２－１のIDが、「UCPのID」には、UCPＡのIDが、「UCPの有効期限」には、UCPＡの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ３－１のIDが、「PTのID」には、PTＡ－１のIDが、そして「PTの有効期限」には、PTＡ－１の有効期限が、それぞれ設定されている。

【０１３５】

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSＡの「UCSのID」には、UCSＡのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSＡの「SAMのID」には、レシーバ５１のSAM６２のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSＡの「ユーザのID」には、ユーザＦのIDが設定されている。

【０１３６】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」などの項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容１１」の「ID１１」に設定されている情報（利用内容１１のID）が、「形式」には、「利用内容１１」の「形式１１」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容１１」の「パラメータ１１」に設定されている情報（”買い取り再生”に対応する情報）が設定される。

【０１３７】

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDと管理移動先の機器のIDは、共に、管理移動元の機器のIDとされる。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には、”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容１１」の「管理移動許可情報１１」に”可”が設定されており、また、このとき、コンテンツＡは管理移動されていないので、SAM６２のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

【０１３８】

「利用履歴」には、同一のコンテンツに対する利用履歴が含まれている。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ５１において、コンテンツＡが以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

【０１３９】

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上

述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【０１４０】

作成されたUCSは、レシーバ５１の復号／暗号化モジュール７４の復号化ユニット９１から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）とともに、外部記憶部６３に送信され、その利用情報記憶部６３Ａに記憶される。外部記憶部６３の利用情報記憶部６３Ａは、図２９に示すように、Ｍ個のブロックＢＰ－１乃至ＢＰ－Ｍに分割され（例えば、１メガバイト毎に分割され）、各ブロックＢＰが、Ｎ個の利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに分割されている。SAM６２から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSは、利用情報用記憶部６３Ａの所定のブロックＢＰの利用情報用メモリ領域ＲＰに、対応して記憶される。

【０１４１】

図２９の例では、ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に、図２８に示したUCSAと、コンテンツＡを復号するためのコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）が対応して記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－１，ＲＰ－２には、他のコンテンツ鍵Ｋｃｏ１，Ｋｃｏ２（それぞれ保存用鍵Ｋｓａｖｅで暗号化されている）およびUCS１，２がそれぞれ記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－４（図示せず）乃至ＲＰ－Ｎ、およびブロックＢＰ－２（図示せず）乃至ＢＰ－Ｍには、コンテンツ鍵ＫｃｏおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域ＲＰに記憶されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

【０１４２】

図３０は、図２８に示したUCSAと同時に作成された課金情報Ａを表している

。課金情報には、図３０に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」などの項目に設定される情報が含まれている。

【０１４３】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定されている。すなわち、図３０の課金情報Ａの、「コンテンツのID」には、コンテンツＡのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ２－１のIDが、「UCPのID」には、UCPＡのIDが、「UCPの有効期限」には、UCPＡの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ３－１のIDが、「PTのID」には、PTＡ－１のIDが、「PTの有効期限」には、PTＡ－１の有効期限が、「UCSのID」には、UCSＡのIDが、「SAMのID」には、SAM６２のIDが、「ユーザのID」には、ユーザＦのIDが、そして「利用内容」には、UCSＡの「利用内容１１」の内容が、それぞれ設定されている。

【０１４４】

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報などが設定される。課金情報Ａの「課金履歴」には、レシーバ５１において計上された課金の合計額が設定されている。

【０１４５】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダ

を特定することができる場合、それを設けないようにすることもできる。

【０１４６】

図２６に戻り、記憶モジュール７３には、図３１に示すように、SAM６２の公開鍵Ｋｐｕ、SAM６２の秘密鍵Ｋｓｕ、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３月分の配送用鍵Ｋｄなどの各種鍵、SAM６２の証明書（図２７）、課金情報（例えば、図３０の課金情報Ａなど）、基準情報５１、およびM個の検査値HP－１乃至HP－Mなどが記憶されている。

【０１４７】

図３２は、記憶モジュール７３に記憶されている基準情報５１を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報などが含まれている。

【０１４８】

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の項目には、EMDサービスセンタ１のユーザ管理部１８により管理されるシステム登録情報（図９）の、それらに対応する項目の情報が設定される。すなわち、基準情報５１には、SAM６２のID、SAM６２の機器番号（１００番）、ユーザＦの決済ID、ユーザＦの決済ユーザ情報（ユーザＦのユーザ一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザＦのID、およびユーザＦのパスワード）、および図３３に示す利用ポイント情報（図１０（Ａ）に示したものと同様の情報）が設定されている。

【０１４９】

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる額が、課金の上限額として設定される。基準情報５１の「課金の上限額」には、レシーバ５１が正式登録されているので、正式登録されている状態における課金の上限額”正式登録時の上限額”）が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録さ

れている状態における課金の上限額よりも、大きな額である。

【０１５０】

次に、記憶モジュール７３に記憶される、図３１に示したM個の検査値HP－１乃至HP－Mについて説明する。検査値HP－１は、外部記憶部６３の利用情報記憶部６３Ａ（図２９）のブロックＢＰ－１に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP－２乃至HP－Mも、検査値HP－１と同様に、外部記憶部６３の、対応するブロックＢＰ－２乃至ＢＰ－Mのそれぞれに記憶されているデータのハッシュ値である。

【０１５１】

図２６に戻り、SAM６２の復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、必要に応じて（例えば、相互認証時）、所定の桁数の乱数を発生して一時鍵Ｋｔｅｍｐを生成し、暗号化ユニット９３に出力する。

【０１５２】

暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、記憶モジュール７３に保持されている保存用鍵Ｋｓａｖｅで暗号化する。暗号化されたコンテンツ鍵Ｋｃｏは、外部記憶部６３に供給される。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６４に送信するとき、コンテンツ鍵Ｋｃｏを乱数発生ユニット９２で生成した一時鍵Ｋｔｅｍｐで暗号化する。

【０１５３】

データ検査モジュール７５は、記憶モジュール７３に記憶されている検査値HPと、外部記憶部６３の利用情報記憶部６３Ａの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査する。データ検査モジュー７５はまた、コンテンツの購入、移動、および管理移動等が行われる際に、検査値HPを再算出し、記憶モジュール７３に記憶（更新）させる。

【０１５４】

伸張部６４は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、SAM６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、HDD５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにレシーバ５１を特定するための情報（例えば、SAM６２のID）のウォータマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

【０１５５】

通信部６５は、ユーザホームネットワーク５のレシーバ２０１との通信処理を行う。インターフェース６６は、SAM６２および伸張部６４からの信号を所定の形式に変更し、HDD５２に出力し、また、HDD５２からの信号を所定の形式に変更し、SAM６２および伸張部６４に出力する。

【０１５６】

表示制御部６７は、表示部（図示せず）への出力を制御する。入力制御部６８は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

【０１５７】

HDD５２は、サービスプロバイダ３から供給されたコンテンツ、UCP、およびPTの他、図３４に示すような、登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【０１５８】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ５１のSAM６２のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶さ

れ、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ５１には、他の機器が接続されていないので、自分自身を含む値１が（「接続されている機器数」の欄に）記憶されている。

【０１５９】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の９個の項目から構成され、この例の場合、レシーバ５１の登録条件として、それぞれの項目に所定の情報が記憶されている。

【０１６０】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ５１のSAM６２のIDが記憶されている。「ユーザID」には、対応する機器のユーザのIDが記憶される。この例の場合、ユーザＦのIDが記憶されている。

【０１６１】

「購入処理」には、コンテンツを購入するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１は、コンテンツを購入するための処理を行うことができるので、”可”が記憶されている。

【０１６２】

「課金処理」には、EMDサービスセンタ１との間で、課金を決済する処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１は、ユーザＦが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、”可”が記憶されている。

【０１６３】

「課金機器」には、計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ５１（SAM６２）は、自分自身が、課金を決済することができるので、SAM６２のIDが記憶されている。

【０１６４】

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ３からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ５１は、コンテンツの供給をサービスプロバイダ３から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

【０１６５】

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合や、正式登録されるための与信処理が完了していない場合（仮登録されている場合）、「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

【０１６６】

この例の場合、レシーバ５１に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

【０１６７】

「登録条件署名」には、登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ１による署名が記憶されている。この例の場合、レシーバ５１の登録条件に対する署名が記憶されている。「登録リスト署名」には、登録リストに設定されたデータの全体に対する署名が設定されている。

【０１６８】

図３５は、レシーバ２０１の構成例を表している。レシーバ２０１の通信部２１１乃至入力制御部２１８は、レシーバ５１の通信部６１乃至入力制御部６８と同様の機能を有しているので、その説明は適宜省略する。

【０１６９】

SAM２１２の記憶モジュール２２３にも、図３６に示すように、SAM２１２の公開鍵Ｋｐｕ、SAM２１２の秘密鍵Ｋｓｕ、EMDサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３月分の配送用鍵Ｋｄ、予め認証局から配布されているSAM２１２の証明書、および基準情報２０１が記憶されている。基準情報２０１には、図３７に示すように、SAM２１２のID、レシーバ２０１の機器番号（１００番）、ユーザＡの決済ID、ユーザＡの決済ユーザ情報（ユーザＡのユーザ一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザＡのID、およびユーザＡのパスワード）、および図３８に示す利用ポイント情報（図１０（Ｂ）に示したものと同様の情報）が設定されている。

【０１７０】

HDD２０２は、HDD５２と同様の機能を有するので、その説明は省略する。

【０１７１】

次に、EMDシステムの処理について、図３９のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ２－１に保持されているコンテンツＡが、サービスプロバイダ３－１を介して、ユーザホームネットワーク５のレシーバ５１に供給され、利用される場合を例として説明する。

【０１７２】

ステップＳ１１において、配送用鍵Ｋｄが、EMDサービスセンタ１からコンテンツプロバイダ２－１に供給される処理が行われる。この処理の詳細は、図４０のフローチャートに示されている。すなわち、ステップＳ３１において、EMDサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２－１の相互認証部３９と相互認証し、コンテンツプロバイダ２－１が、正当なプロバイダであることが確認した後、EMDサービスセンタ１のコンテンツプロバイダ管理部１２は、鍵サーバ１４から供給された配送用鍵Ｋｄをコンテンツプロバイダ２－１に送信

する。なお、相互認証処理の詳細は、図４１乃至図４３を参照して後述する。

【０１７３】

次に、ステップＳ３２において、コンテンツプロバイダ２－１の暗号化部３６は、EMDサービスセンタ１から送信された配送用鍵Ｋｄを受信し、ステップＳ３３において、記憶する。

【０１７４】

このように、コンテンツプロバイダ２－１の暗号化部３６が、配送用鍵Ｋｄを記憶したとき、処理は終了し、図３９のステップＳ１２に進む。ここで、ステップＳ１２以降の処理の説明の前に、図４０のステップＳ３１における相互認証処理（なりすましがないことを確認する処理）について、１つの共通鍵を用いる場合（図４１）、２つの共通鍵を用いる場合（図４２）、および公開鍵暗号を用いる場合（図４３）を例として説明する。

【０１７５】

図４１は、１つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋｃで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１７６】

ステップＳ４４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃで復号する。ステップＳ４５において、EMDサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、EMDサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ビットを表し、Ａ‖Ｂは、

ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、EMDサービスセンタ１の相互認証部１７は、DESを用いて$Ｒ１_{Ｈ}$‖Ｒ２を共通鍵Ｋｃで暗号化する。ステップＳ４８において、EMDサービスセンタ１の相互認証部１７は、暗号化した$Ｒ１_{Ｈ}$‖Ｒ２をコンテンツプロバイダ２に送信する。

【０１７７】

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$Ｒ１_{Ｈ}$‖Ｒ２を共通鍵Ｋｃで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$Ｒ１_{Ｈ}$‖Ｒ２の上位３２ビット$Ｒ１_{Ｈ}$を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$Ｒ１_{Ｈ}$と一致すれば、EMDサービスセンタ１が正当なセンタであることを認証する。生成した乱数$Ｒ１_{Ｈ}$と、受信した$Ｒ１_{Ｈ}$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信し、復号した３２ビットの乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋｃで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１７８】

ステップＳ５５において、EMDサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Ｋｃで復号する。ステップＳ５６において、EMDサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【０１７９】

図４２は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部

１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、DESを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をEMDサービスセンタ１に送信する。

【０１８０】

ステップＳ６４において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、EMDサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、EMDサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１８１】

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、EMDサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をEMDサービスセンタ１に送信する。

【０１８２】

ステップＳ７３において、EMDサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、EMDサービス

センタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【０１８３】

図４３は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とEMDサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）と、乱数Ｒ１をEMDサービスセンタ１の相互認証部１７に送信する。

【０１８４】

ステップＳ８３において、EMDサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【０１８５】

適正な認証結果が得られたとき、ステップＳ８４において、EMDサービスセン

タ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、EMDサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、EMDサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、EMDサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

【０１８６】

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、EMDサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればEMDサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【０１８７】

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得

した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をEMDサービスセンタ１の相互認証部１７に送信する。

【０１８８】

ステップＳ９７において、EMDサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、EMDサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【０１８９】

以上のように、EMDサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

【０１９０】

次に、図３９のステップＳ１２の処理について説明する。ステップＳ１２においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ２－１からサービスプロバイダ３－１に供給される処理が行われる。その処理の詳細は、図４４のフローチャートに示されている。すなわち、ステップＳ２０１において、コンテンツプロバイダ２－１のウォータマーク付加部３２は、コンテンツサーバ３１からコンテンツＡを読み出し、コンテンツプロバイダ２－１を示す所定のウォータマーク（電子透かし）を挿入し、圧縮部３３に供給する。

【０１９１】

ステップＳ２０２において、コンテンツプロバイダ２－１の圧縮部３３は、ウォータマークが挿入されたコンテンツＡをATRAC2等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２０３において、乱数発生部３５は、コンテンツ鍵ＫｃｏＡとなる乱数を発生させ、暗号化部３４に供給する。

【０１９２】

ステップＳ２０４において、コンテンツプロバイダ２－１の暗号化部３４は、DESなどの所定の方式で、乱数発生部３５で発生された乱数（コンテンツ鍵ＫｃｏＡ）を使用して、ウォータマークが挿入されて圧縮されたコンテンツＡを暗号化する。次に、ステップＳ２０５において、暗号化部３６は、DESなどの所定の方式で、EMDサービスセンタ１から供給された配送用鍵Ｋｄでコンテンツ鍵ＫｃｏＡを暗号化する。

【０１９３】

ステップＳ２０６において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびポリシー記憶部３７に記憶されている、コンテンツＡに対応するUCPA，Ｂ（図１２）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化する。これにより、図１７に示した署名が作成される。

【０１９４】

ステップＳ２０７において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、UCPA，Ｂ（図１２）、およびステップＳ２０６で生成した署名を含んだ、図１７に示したコンテンツプロバイダセキュアコンテナを作成する。

【０１９５】

ステップＳ２０８において、コンテンツプロバイダ２－１の相互認証部３９は、サービスプロバイダ３－１の相互認証部４５と相互認証する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、その説明は省略する。ステップＳ２０９において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、認証局から予め発行された証明書（図１８）を、ステップＳ２０７で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ３－１に送信する。

【０１９６】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ３－１に供給されたとき、処理は終了し、図３９のステップＳ１３に進む。

【０１９７】

ステップＳ１３において、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からユーザホームネットワーク５（レシーバ５１）に供給される。この処理の詳細は、図４５のフローチャートに示されている。すなわち、ステップＳ２２１において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図１８）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図４３のステップＳ８３における処理と同様であるので、その説明は省略する。

【０１９８】

ステップＳ２２２において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２－１の公開鍵Ｋｐｃｐで復号し、得られたハッシュ値が、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびUCPA，Ｂの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップＳ２２３に進む。

【０１９９】

ステップＳ２２３において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダセキュアコンテナから、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、および署名を取り出し、コンテンツサーバ４１に供給する。コンテンツサーバ４１は、それらを記憶する。値付け部４２はまたUCPA，Ｂも、コンテン

ツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部４４に供給する。

【０２００】

ステップＳ２２４において、サービスプロバイダ３－１の値付け部４２は、取り出したUCPA，Bに基づいて、PTA－１，Ａ－２（図２０）、およびPTＢ－１，Ｂ－２（図２２）を作成し、セキュアコンテナ作成部４４に供給する。

【０２０１】

ステップＳ２２５において、サービスプロバイダ３－１のセキュアコンテナ作成部４４は、コンテンツサーバ４１から読み出したコンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツプロバイダ２の署名、値付け部４２から供給された、UCPA，Ｂ、およびPTＡ－１，Ａ－２，Ｂ－１，Ｂ－２、並びにその署名から、図２４に示したサービスプロバイダセキュアコンテナを作成する。

【０２０２】

ステップＳ２２６において、サービスプロバイダ３－１の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、その説明を省略する。

【０２０３】

ステップＳ２２７において、サービスプロバイダ３－１のセキュアコンテナ作成部４４は、ステップＳ２２５で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ３－１の証明書（図２５）を付して、ユーザホームネットワーク５のレシーバ５１に送信する。

【０２０４】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からレシーバ５１に送信されたとき、処理は終了し、図３９のステップＳ１４に進む。

【０２０５】

ステップＳ１４において、サービスプロバイダ３－１から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク５のレシーバ５１に

より受信される。この処理の詳細は、図４６のフローチャートに示されている。すなわち、ステップＳ２４１において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、サービスプロバイダ３－１の相互認証部４５と相互認証し、相互認証できたとき、通信部６１は、相互認証したサービスプロバイダ３－１から、サービスプロバイダセキュアコンテナ（図２４）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップＳ２４２に進む。

【０２０６】

ステップＳ２４２において、レシーバ５１の通信部６１は、ステップＳ２４１で相互認証したサービスプロバイダ３－１から、公開鍵証明書を受信する。

【０２０７】

ステップＳ２４３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ２４１で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップＳ２４４に進む。

【０２０８】

ステップＳ２４４において、UCPおよびPTが選択され、かつ、その利用内容および価格内容が選択される。具体的には、レシーバ５１の記憶モジュール７３に記憶されている基準情報５１（図３２）が、利用条件を満たすUCPと価格条件を満たすPTが選択される。この例の場合、レシーバ５１の基準情報５１の「利用ポイント情報」には、図３３に示したように、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイントであるとされている。すなわち、この基準情報５１によれば、コンテンツＡに対応して設定されたUCPA，Ｂのうち、「利用条件１０」の「ユーザ条件１０」が”２００ポイント以上”とされているUCPＡ（図１２（Ａ））が選択される。また、基準情報５１の「決済ユーザ情報」には、ユーザＦは男性とされているので、PTＡ－１（図２０（Ａ））の「価格条件１０」に設定された条件を満たす。その結果、UCPＡに対応して作成されたPTＡ－１，PTＡ－２のうち、PTＡ－１が選択される。

【０２０９】

その後、このようにして選択されたUCPAおよびPTA－１の内容が、表示制御部６７を介して、図示せぬ表示部に表示される。そこで、ユーザFは、その表示を参照して（例えば、利用したい利用形式と、その価格を比較検討して）、UCPAの所定の「利用内容」を選択するための操作を、図示せず操作部に対して行う。これにより、入力制御部６８を介して、選択されたUCPAの利用内容のIDおよびPTA－１のIDがSAM６２に出力される。なお、この例の場合、UCPAの利用内容１１（PTA－１の価格内容１１）が選択されたものとする。

【０２１０】

ステップＳ２４５において、レシーバ５１のSAM６２の課金処理モジュール７２は、ステップＳ２４４で選択された、UCPAの「利用内容１１」とPTA－１に基づいて、UCSA（図２８）および課金情報A（図３０）を作成する。すなわち、この場合、コンテンツAは、料金が２０００円で買い取り再生される。

【０２１１】

ステップＳ２４６において、サービスプロバイダセキュアコンテナ（図２４）に含まれる、コンテンツA（コンテンツ鍵ＫｃｏAで暗号化されている）、UCPA、PTA－１，A－２、およびコンテンツプロバイダ２の署名が取り出され、HDD５２に出力され、記憶される。ステップＳ２４７において、復号／暗号化ユニット７４の復号ユニット９１は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵ＫｃｏA（配送用鍵Ｋｄで暗号化されている）を、記憶モジュール７３に記憶されている配送用鍵Ｋｄで復号する。

【０２１２】

ステップＳ２４８において、復号／暗号化ユニット７４の暗号化ユニット９３は、ステップＳ２４７で復号されたコンテンツ鍵ＫｃｏAを、記憶モジュール７３に記憶されている保存用鍵Ｋｓａｖｅで暗号化する。

【０２１３】

ステップＳ２４９において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４８で保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏA、およびステップＳ２４５で作成されたUCSAが対応して記憶される、外部記憶部６

３の利用情報記憶部６３Ａ（図２９）のブロックBPを検出する。この例の場合、利用情報記憶部６３ＡのブロックBP－１が検出される。なお、図２９の利用情報記憶部６３Ａにおいて、そのブロックBP－１の利用情報用メモリ領域RP－３にコンテンツ鍵ＫｃｏＡおよびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、空いることを示す所定の初期情報が記憶されている。

【０２１４】

ステップＳ２５０において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４９で検出したブロックBP－１のデータ（利用情報用メモリ領域RP－１乃至RP－Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップＳ２５１において、データ検査モジュール７５は、ステップＳ２５０で得られたハッシュ値と、記憶モジュール７３に記憶されているブロックBP－１に対応する検査値HP－１（図３１）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP－１のデータは改竄されていないので、ステップＳ２５２に進む。

【０２１５】

ステップＳ２５２において、レシーバ５１のSAM６２は、利用情報（ステップＳ２４８で、保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたUCSA）を、外部記憶部６３のブロックBP－１の利用情報用メモリ領域RP－３に記憶させる。

【０２１６】

ステップＳ２５３において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２５２で利用情報が記憶された利用情報用メモリ領域RP－３が属する、利用情報記憶部６３ＡのブロックBP－１に記憶されている全てのデータにハッシュ関数を適用してハッシュ値を算出し、ステップＳ２５４において、記憶モジュール７３に記憶されている検査値HP－１に上書きする。ステップＳ２５５において、課金処理モジュール７２は、ステップＳ２４５で作成した課金情報Ａを記憶モジュール７３に記憶させ、処理は終了する。

【０２１７】

ステップＳ２５１において、算出されたハッシュ値と検査値HP－１とが一致しないと判定された場合、ブロックBP－１のデータは改竄されているので、手続きは、ステップＳ２５６に進み、データ検査モジュール７５は、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックBPを調べたか否かを判定し、外部記憶部６３の全てのブロックBPを調べていないと判定した場合、ステップＳ２５７に進み、利用情報記憶部６３Ａの、空きを有する他のブロックBPを検索し、ステップＳ２５０に戻り、それ以降の処理が実行される。

【０２１８】

ステップＳ２５６において、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックBPが調べられたと判定された場合、利用情報を記憶できるブロックBP（利用情報用メモリ領域RP）は存在しないので、処理は終了する。

【０２１９】

このように、サービスプロバイダセキュアコンテナが、レシーバ５１により受信されると、処理は終了し、図３９のステップＳ１５に進む。

【０２２０】

ステップＳ１５において、供給されたコンテンツＡが、レシーバ５１において利用される。なお、この例の場合選択されたUCPAの利用内容１１によれば、コンテンツＡは、再生して利用される。そこで、ここでは、コンテンツＡの再生処理について説明する。この再生処理の詳細は、図４７のフローチャートに示されている。

【０２２１】

ステップＳ２６１において、レシーバ５１のデータ検査モジュール７５は、図４６のステップＳ２５２で、コンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）およびUCSAが記憶された利用情報用メモリ領域RP－３が属する、外部記憶部６３の利用情報記憶部６３ＡのブロックBP－１のデータにハッシュ関数を適用してハッシュ値を算出する。

【０２２２】

ステップＳ２６２において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２６１において算出したハッシュ値が、図４６のステップＳ２５３で算

出し、ステップＳ２５４で記憶モジュール７３に記憶させたハッシュ値（検査値HP－１）と一致するか否かを判定し、一致すると判定した場合、ブロックBP－１のデータは改竄されていないので、ステップＳ２６３に進む。

【０２２３】

ステップＳ２６３において、UCSA（図２８）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツＡが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、”期間制限再生”とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。現在の時刻がその範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が０回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が０回であるとき、利用不可と判定される。

【０２２４】

なお、UCSAの「利用内容」の「形式」は、”買い取り再生”とされているので、この場合、コンテンツＡは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップＳ２６３において、コンテンツＡが利用可能であると判定され、ステップＳ２６４に進む。

【０２２５】

ステップＳ２６４において、レシーバ５１の課金モジュール７２は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が１つだけデクリメントされる。

【０２２６】

次に、ステップＳ２６５において、レシーバ５１のSAM６２は、ステップＳ２６４で更新されたUCSA（実際は、更新されていない）を、外部記憶部６３の利用情報記憶部６３Ａのブロック BP－１の利用情報用メモリ領域RP－３に記憶させる。ステップＳ２６６において、データ検査モジュール７５は、ステップＳ２６５でUCSAが記憶された、外部記憶部６３の利用情報記憶部６３Ａのブロック BP－１のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール７３に記憶されている検査値HP－１に上書きする。

【０２２７】

ステップＳ２６７において、SAM６２の相互認証モジュール７１と、伸張部６４の相互認証モジュール１０１は、相互認証し、SAM６２および伸張部６４は、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。

【０２２８】

ステップＳ２６８において、復号／暗号化モジュール７４の復号ユニット９１は、図４６のステップＳ２５２で外部記憶部６３の利用情報記憶部６３Ａのブロック BP－１（利用情報用メモリ領域RP－３）に記憶されたコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）を、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。

【０２２９】

次に、ステップＳ２６９において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ２７０において、SAM６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵ＫｃｏＡを伸張部６４に送信する。

【０２３０】

ステップＳ２７１において、伸張部６４の復号モジュール１０２は、コンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで復号する。ステップＳ２７２において、伸張

部６４は、インタフェース６６を介して、HDD５２に記録されたコンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）を受け取る。ステップＳ２７３において、伸張部６４の復号モジュール１０３は、コンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）をコンテンツ鍵ＫｃｏＡで復号する。

【０２３１】

ステップＳ２７４において、伸張部６４の伸張モジュール１０４は、復号されたコンテンツＡをATRAC2などの所定の方式で伸張する。ステップＳ２７５において、伸張部６４のウォータマーク付加モジュール１０５は、伸張されたコンテンツＡにレシーバ５１を特定する所定のウォータマーク（電子透かし）を挿入する。ステップＳ２７６において、コンテンツＡは、図示せぬスピーカなどに出力され、再生される。その後、処理は終了する。

【０２３２】

ステップＳ２６２において、ステップＳ２６１において算出されたハッシュ値が、レシーバ５１の記憶モジュール７３に記憶された検査値ＨＰ－１と一致しないと判定された場合、またはステップＳ２６３において、コンテンツが利用不可と判定された場合、ステップＳ２７７において、SAM６２は、表示制御部６７を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【０２３３】

このようにして、レシーバ５１において、コンテンツＡが再生（利用）されたとき、処理は終了し、図３９の処理も終了する。

【０２３４】

なお、以上においては、コンテンツＡが、レシーバ５１において利用（購入）される場合を例として説明したが、レシーバ２０１も、レシーバ５１と同様に、コンテンツＡを利用することができる。ただし、レシーバ２０１の基準情報２０１の「利用ポイント情報」には、図３８に示したように、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２３ポイントとされているので、UCPAの「利用条件１０」の「ユーザ条件１０」の条件を満たさない。すなわち、この場合、UCPAは選択されず、UCPBが選択される。

【０２３５】

次に、PTが選択されるが、この場合、UCPＢが選択されているので、UCPＢに対応するPTＢ－１，Ｂ－２（図２２）のうちのいずれかが選択される。PTＢ－１の「価格条件３０」は、機器が従機器であることが条件とされ、またPTＢ－２の「価格条件４０」は、主機器であることが条件とされている。すなわち、主機器であるレシーバ２０１においては、PTＢ－２が選択される。このように、機器およびそのユーザに設定された各種条件に基づいて、UCP、UCPの利用内容、およびPTの選択範囲が決定される。

【０２３６】

また、以上においては、UCPの「利用条件」またはPTの「価格条件」の「ユーザ条件」を、ユーザの性別や年齢に関する条件とする場合を例として説明したが、例えば、ユーザの住んでいる地域や誕生日などを条件とすることもできる。なお、この場合、図１５（Ａ）のサービスコードの０３００ｈ乃至７ＦＦＦｈのコート値に、それらの条件の意味を設定する。

【０２３７】

次に、レシーバ５１の課金が決済される場合の処理手順を、図４８のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を超えた場合、または配送用鍵Ｋｄのバージョンが古くなり、例えば、図４６のステップＳ２４７で、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

【０２３８】

すなわち、ステップＳ３０１において、レシーバ５１とEMDサービスセンタ１との相互認証が行われる。この相互認証は、図４１乃至図４３を参照して説明した場合と同様の処理であるので、その説明は省略する。

【０２３９】

次に、ステップＳ３０２において、レシーバ５１のSAM６２は、EMDサービスセンタ１のユーザ管理部１８に証明書を送信する。ステップＳ３０３において、レ

シーバ５１のSAM６２は、記憶モジュール７３に記憶されている課金情報を、ステップＳ３０１でEMDサービスセンタ１と共有した一時鍵Ｋｔｅｍｐで暗号化し、配送用鍵Ｋｄのバージョン、HDD５２に記憶されているUCPおよびPT、並びに登録リストとともに、EMDサービスセンタ１に送信する。

【０２４０】

ステップＳ３０４において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３０３で、レシーバ５１から送信された情報を受信し、復号した後、EMDサービスセンタ１のユーザ管理部１８が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ５１において存在するか否かを確認する。

【０２４１】

ステップＳ３０５において、EMDサービスセンタ１の課金請求部１９は、ステップＳ３０３で受信された課金情報を解析し、ユーザ（例えば、ユーザＦ）の支払い金額を算出する処理等を行う。次に、ステップＳ３０６において、ユーザ管理部１８は、ステップＳ３０５における処理により、決済が成功したか否かを確認する。

【０２４２】

次に、ステップＳ３０７において、EMDサービスセンタ１のユーザ管理部１８は、ステップＳ３０４における確認結果、およびステップＳ３０６における確認結果に基づいて、レシーバ５１の登録条件を設定し、それに署名を付して、レシーバ５１の登録リストを作成する。

【０２４３】

例えば、ステップＳ３０４で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップＳ３０６で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【０２４４】

次に、ステップＳ３０８に進み、EMDサービスセンタ１のユーザ管理部１８は、最新バージョンの配送用鍵Ｋｄ（３月分の最新バージョンの配送用鍵Ｋｄ）を一時鍵Ｋｔｅｍｐで暗号化し、ステップＳ３０７で作成された登録リストとともにレシーバ５１に送信する。

【０２４５】

ステップＳ３０９において、レシーバ５１のSAM６２は、EMDサービスセンタ１から送信された配送用鍵Ｋｄおよび登録リストを、通信部６１を介して受信し、復号した後、記憶モジュール７３に記憶させる。このとき、記憶モジュール７３に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Ｋｄが更新される。

【０２４６】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【０２４７】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【０２４８】

【発明の効果】

請求項１に記載の情報処理装置、請求項３に記載の情報処理方法、および請求項４に記載の提供媒体によれば、第１の情報に対応させて、利用条件および利用内容を含む第２の情報を記憶するようにしたので、第１の情報に対応させて第２の情報を所定のプロバイダに送信することができる。

【０２４９】

請求項４に記載の情報処理装置、請求項５に記載の情報処理方法、および請求項６に記載の提供媒体によれば、第１の情報の利用条件および利用内容を含む第２の情報に対応して、第１の情報の価格条件および価格内容を含む第３の情報を作成するようにしたので、第１の情報に対応させて第２の情報および第３の情報を、所定の機器に送信することができる。

【０２５０】

請求項７に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体によれば、基準情報に対応して選択した利用条件に対応する利用内容に従って、コンテンツを利用し、基準情報に対応して選択した価格条件に対応する価格内容に従って、コンテンツの利用に対して、課金処理を実行するようにしたので、変化に富んだサービスを受けることができる。

【図面の簡単な説明】

【図１】

EMDシステムを説明する図である。

【図２】

EMDシステムにおける、主な情報の流れを説明する図である。

【図３】

EMDサービスセンタ１の機能的構成を示すブロック図である。

【図４】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する図である。

【図５】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図６】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図７】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図８】

EMDサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図である。

【図９】

システム登録情報を説明する図である。

【図１０】

利用ポイント情報を説明する図である。

【図１１】

コンテンツプロバイダ２の機能的構成例を示すブロック図である。

【図１２】

UCPの例を示す図である。

【図１３】

コンテンツの管理移動を説明する図である。

【図１４】

第１世代複製を説明する図である。

【図１５】

サービスコードおよびコンディションコードのコード値の例を示す図である。

【図１６】

UCPの利用条件として設定されたコード値の例を示す図である。

【図１７】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図１８】

コンテンツプロバイダ２の証明書の例を示す図である。

【図１９】

サービスプロバイダ３の機能的構成を示すブロック図である。

【図２０】

PTの例を示す図である。

【図２１】

PTの価格条件として設定されたコード値の例を示す図である。

【図２２】

他のPTの例を示す図である。

【図２３】

他のPTの価格条件として設定されたコード値の例を示す図である。

【図２４】

サービスプロバイダセキュアコンテナの例を示す図である。

【図２５】

サービスプロバイダ３の証明書の例を示す図である。

【図２６】

ユーザホームネットワーク５のレシーバ５１の機能的構成例を示すブロック図である。

【図２７】

レシーバ５１のSAM６２の証明書の例を示す図である。

【図２８】

UCSの例を示す図である。

【図２９】

レシーバ５１の外部記憶部６３の利用情報記憶部６３Ａの内部を説明する図である。

【図３０】

課金情報の例を示す図である。

【図３１】

レシーバ５１の記憶モジュール７３に記憶されている情報を示す図である。

【図３２】

基準情報５１を説明する図である。

【図３３】

基準情報５１の利用ポイント情報の例を示す図である。

【図３４】

登録リストの例を示す図である。

【図３５】

ユーザホームネットワーク５のレシーバ２０１の機能的構成例を示すブロック図である。

【図３６】

レシーバ２０１の記憶モジュール２２３に記憶されている情報の例を示す図である。

【図３７】

基準情報２０１の例を示す図である。

【図３８】

基準情報５１の利用ポイント情報の例を示す図である。

【図３９】

コンテンツの利用処理を説明するフローチャートである。

【図４０】

EMDサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

【図４１】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の動作を説明するフローチャートである。

【図４２】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

【図４３】

コンテンツプロバイダ２とEMDサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

【図４４】

コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図４５】

サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図４６】

レシーバ５１がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図４７】

レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

【図４８】

決済処理を説明するフローチャートである。

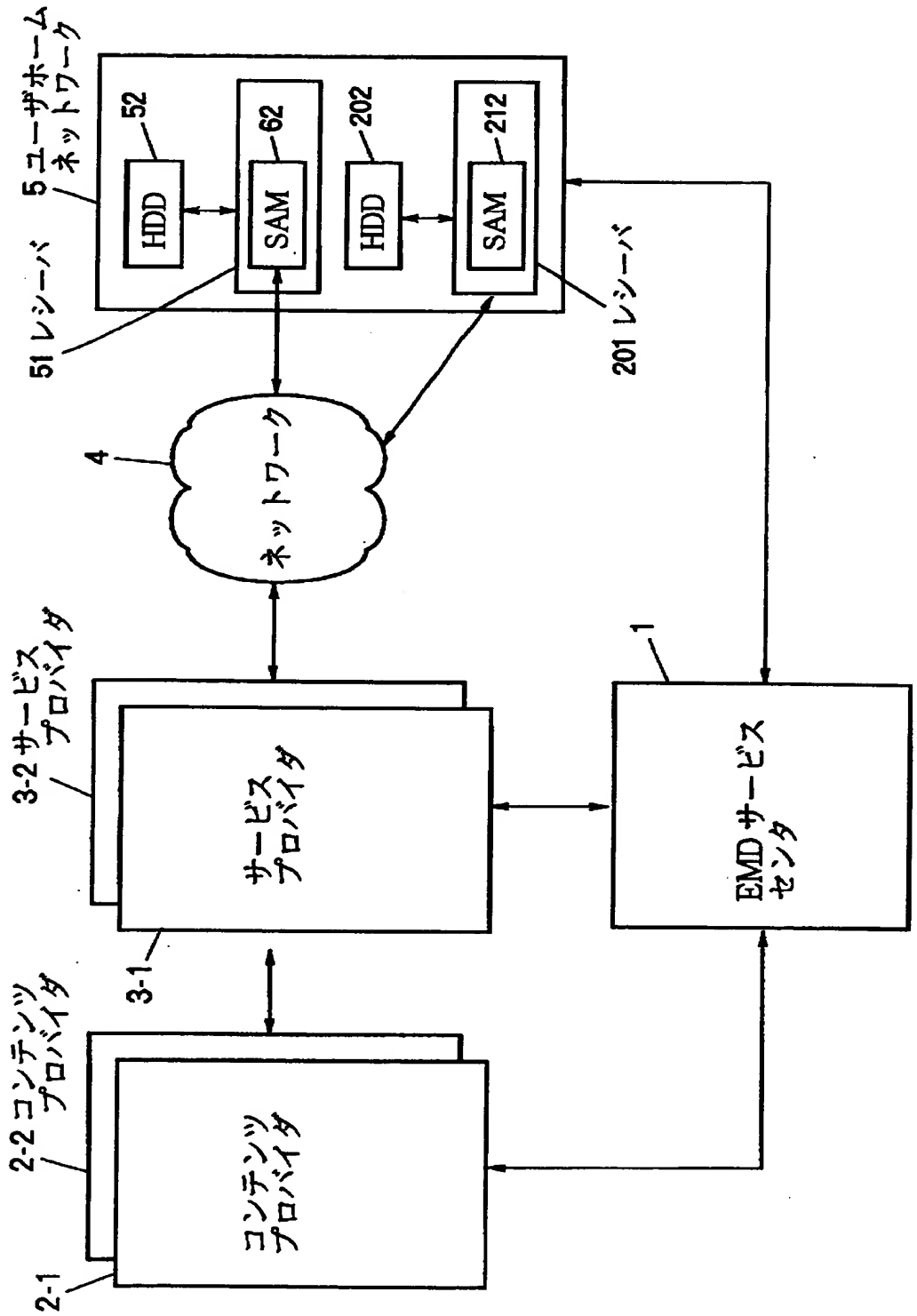
【符号の説明】

１　EMDサービスセンタ，　２　コンテンツプロバイダ，　３　サービスプロ

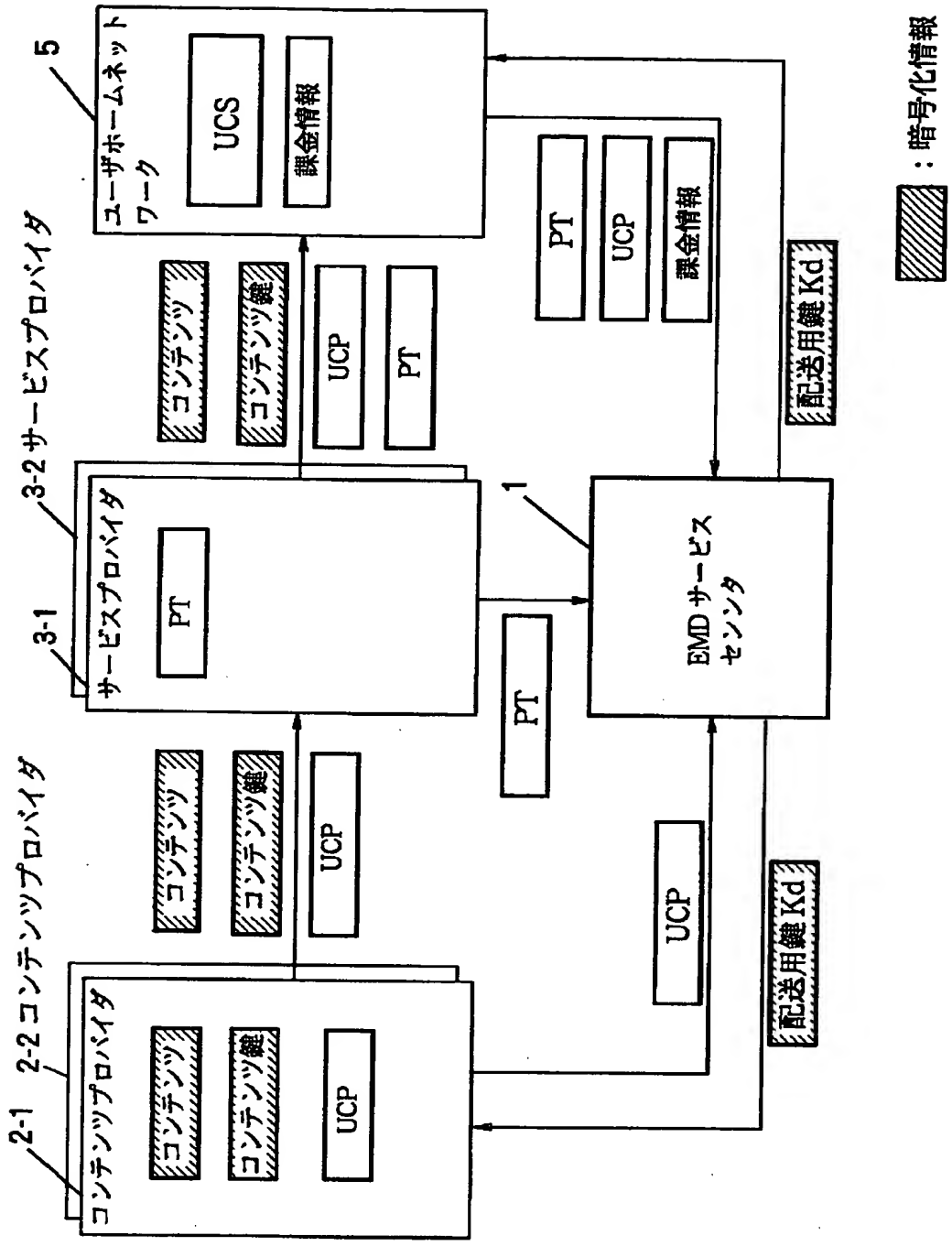
バイダ，　５　ユーザホームネットワーク，　１１　サービスプロバイダ管理部，　１２　コンテンツプロバイダ管理部，　１３　著作権管理部，　１４　鍵サーバ，　１５　経歴データ管理部，　１６　利益分配部，　１７　相互認証部，　１８　ユーザ管理部，　１９　課金請求部，　２０　出納部，　２１　監査部，　３１　コンテンツサーバ，　３２　ウォータマーク付加部，　３３　圧縮部，　３４　暗号化部，　３５　乱数発生部，　３６　暗号化部，　３７　ポリシー記憶部，　３８　セキュアコンテナ作成部，　３９　相互認証部，　４１　コンテンツサーバ，　４２　値付け部，　４３　ポリシー記憶部，　４４　セキュアコンテナ作成部，　４５　相互認証部，　５１　レシーバ，　５２　HDD，　６１　通信部，　６２　SAM，　６３　外部記憶部，　６４　伸張部，　６５　通信部，　６６　インタフェース，　６７　表示制御部，　６８　入力制御部，　７１　相互認証モジュール，　７２　課金処理モジュール，　７３　記憶モジュール，　７４　復号／暗号化モジュール，　７５　データ検査モジュール，　９１　復号ユニット，　９２　乱数発生ユニット，　９３　暗号化ユニット，　１０１　相互認証モジュール，　１０２　復号モジュール，　１０３　復号モジュール，　１０４　伸張モジュール，　１０５　ウォータマーク付加モジュール，　２０１　レシーバ，　２０２　HDD，　２１１　通信部，　２１２　SAM，　２１３　外部記憶部，　２１４　伸張部，　２１５　通信部，　２１６　インタフェース，　２１７　表示制御部，　２１８　入力制御部，　２２１　相互認証モジュール，　２２２　課金処理モジュール，　２２３　記憶モジュール，　２２４　復号／暗号化モジュール，　２２５　データ検査モジュール，　２３１　復号ユニット，　２３２　乱数発生ユニット，　２３３　暗号化ユニット，　２４１　相互認証モジュール，　２４２　復号モジュール，　２４３　復号モジュール，　２４４　伸張モジュール，　２４５　ウォータマーク付加モジュール

【書類名】　図面

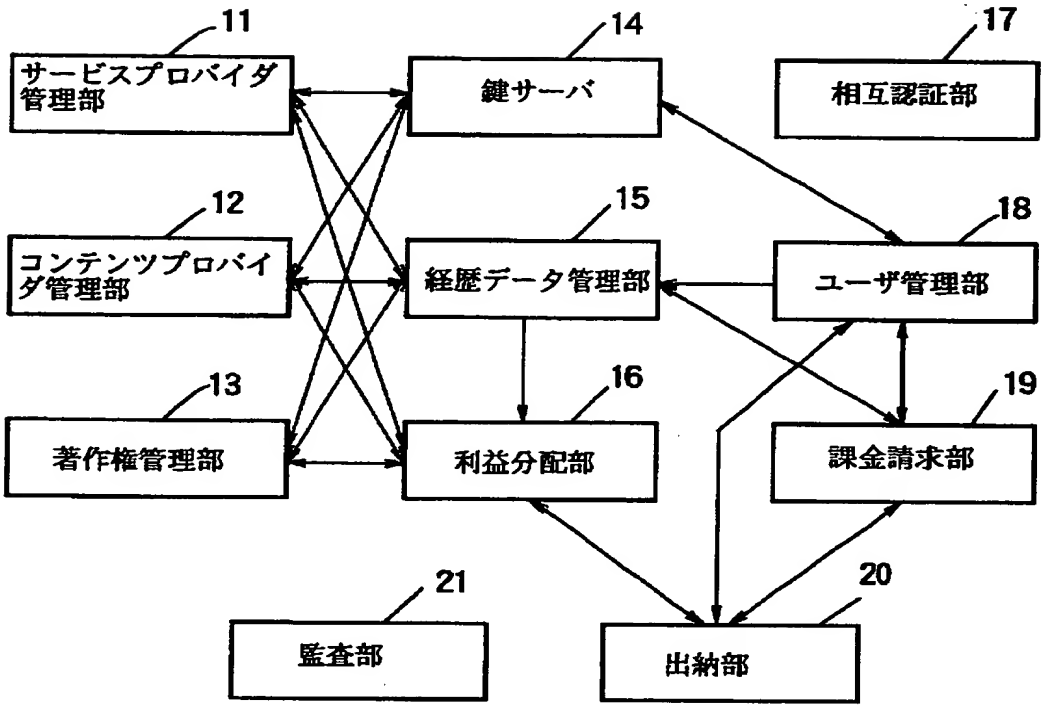
【図１】


5 ユーザホーム ネットワーク
52
HDD
62
SAM
202
HDD
212
SAM
51 レシーバ
201 レシーバ
4
ネットワーク
3-2 サービス プロバイダ
サービス プロバイダ
3-1
1
EMD サービス センタ
2-2 コンテンツ プロバイダ
コンテンツ プロバイダ
2-1

【図２】

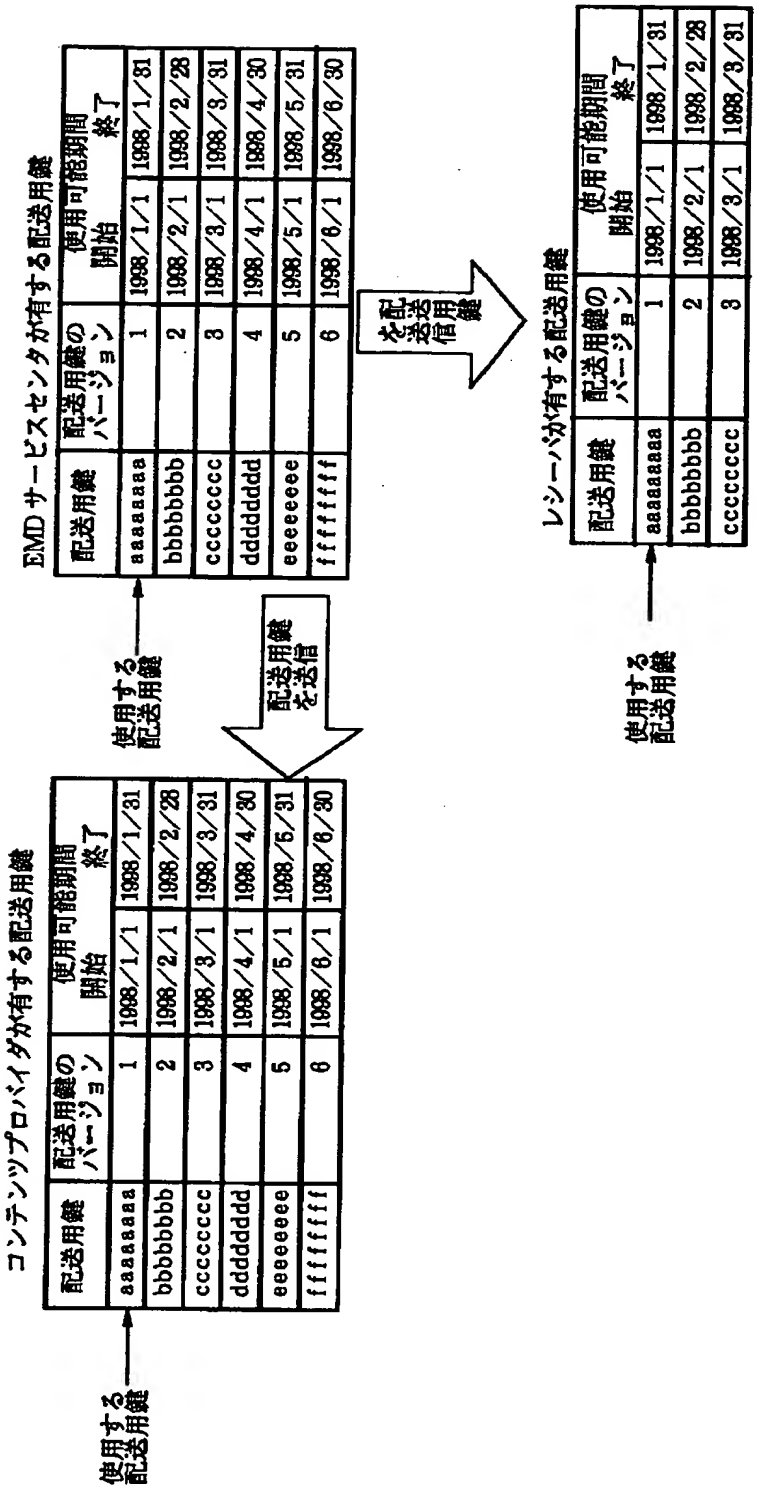

5
ユーザホームネットワーク
UCS
課金情報
3-2 サービスプロバイダ
コンテンツ
コンテンツ鍵
UCP
PT
3-1
サービスプロバイダ
PT
1
EMD サービスセンタ
PT
UCP
課金情報
配送用鍵 Kd
2-1 2-2 コンテンツプロバイダ
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
UCP
UCP
配送用鍵 Kd
：暗号化情報

【図３】

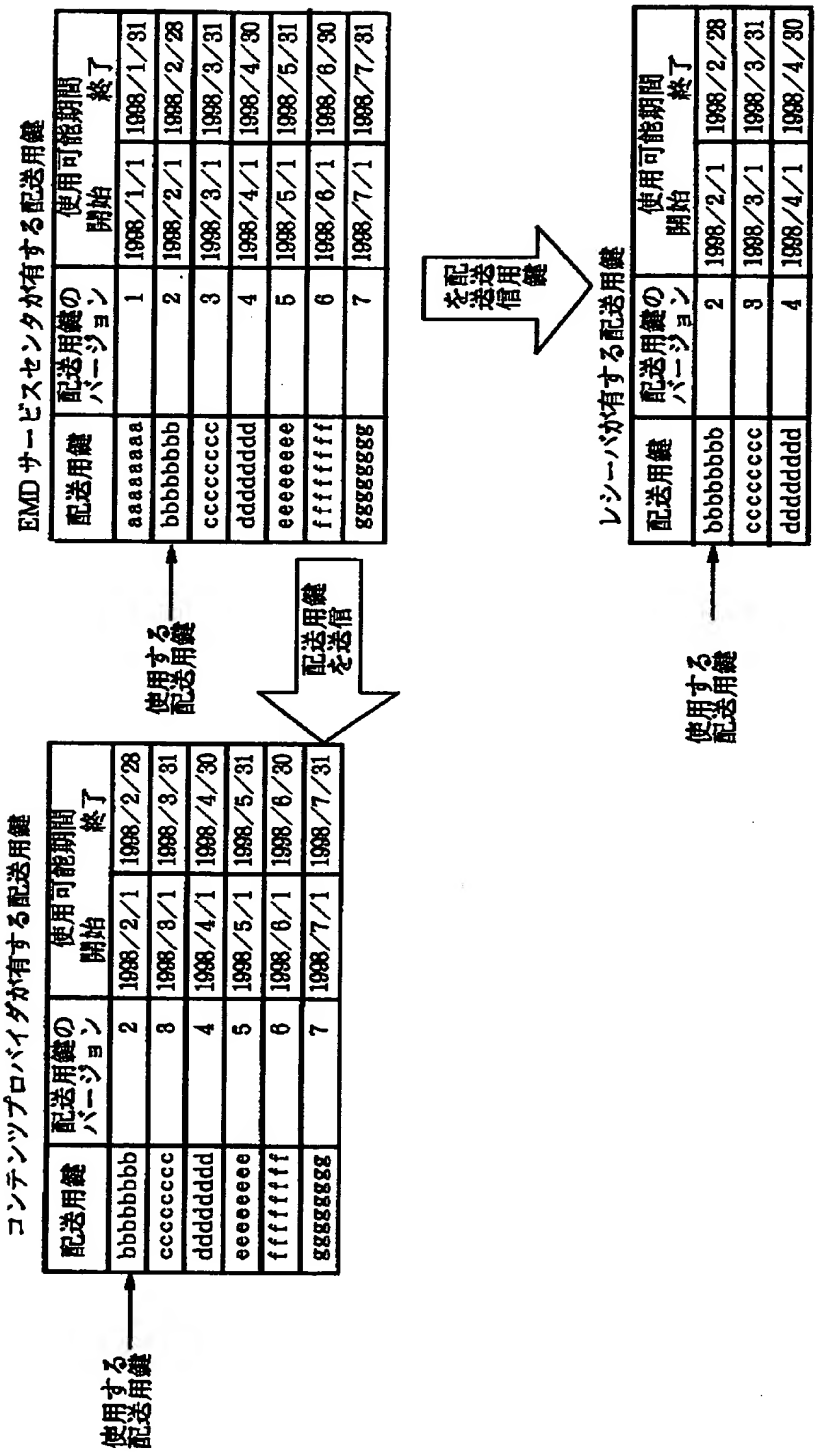


EMD サービスセンタ 1

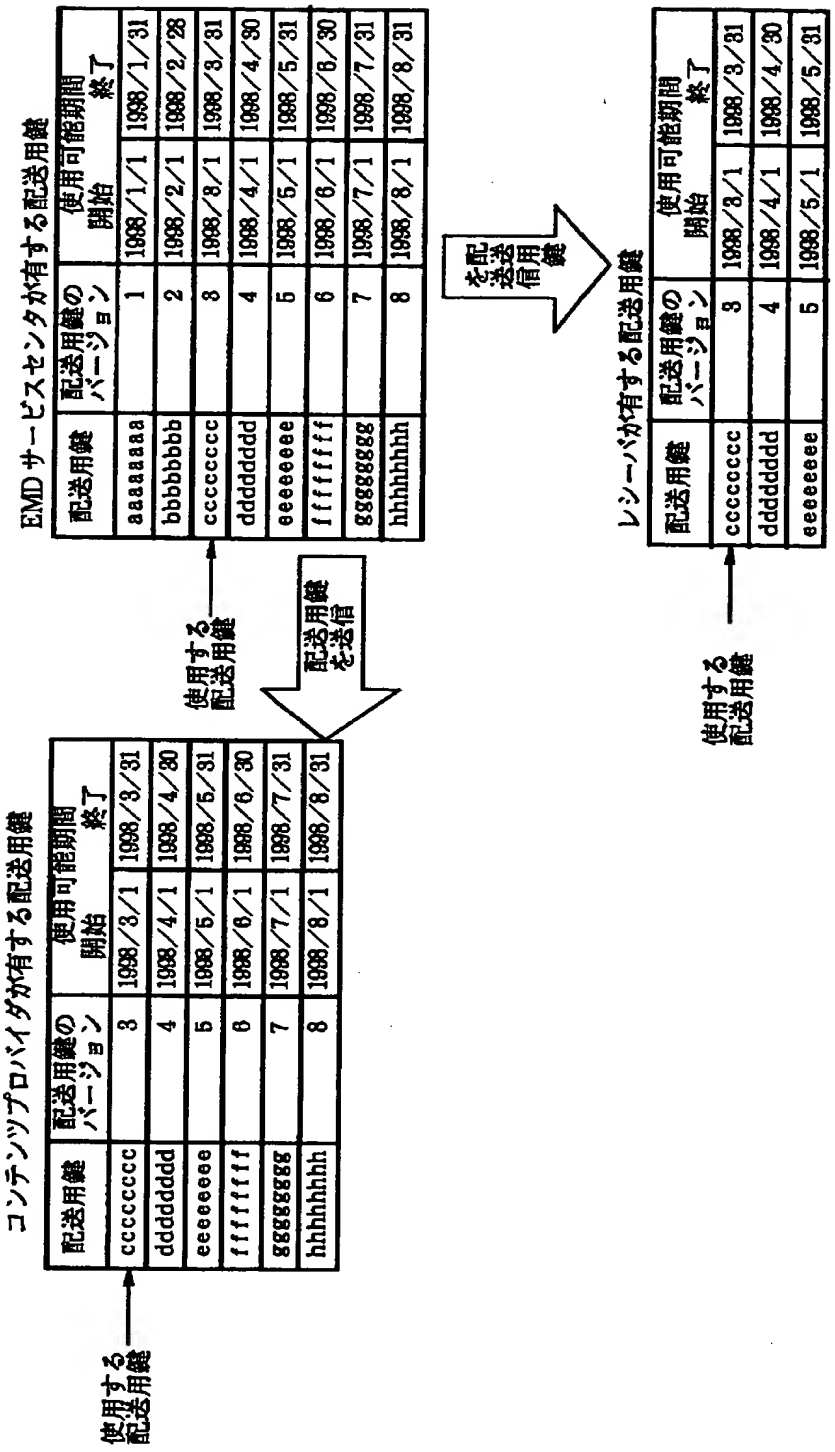
【図４】


コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
配送用鍵を送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

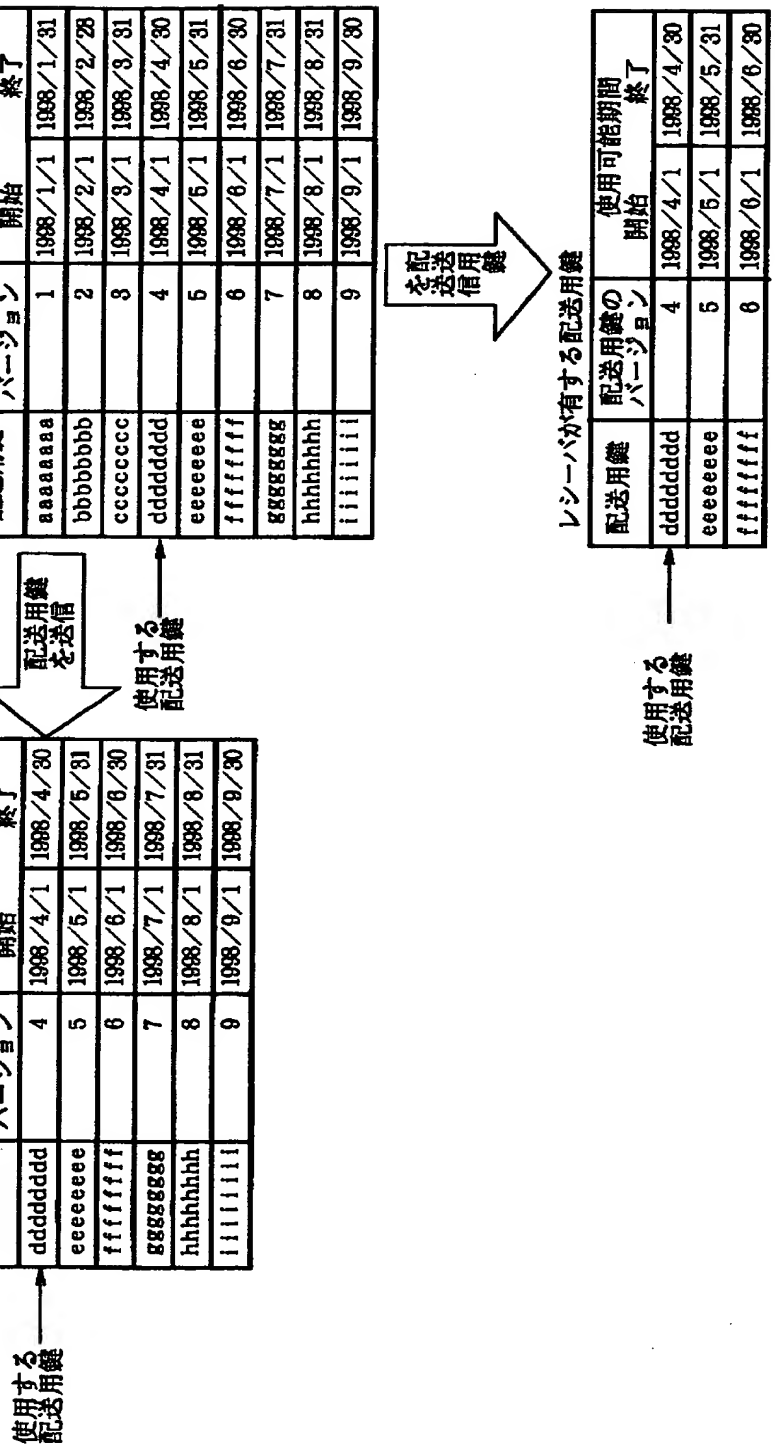
【図５】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
配送用鍵を送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

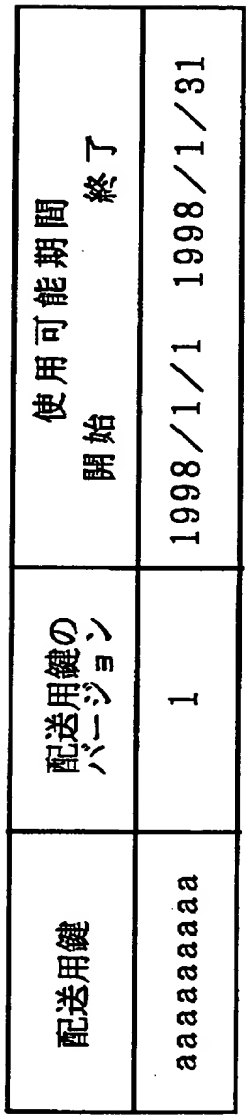
【図６】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を送信
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
使用する配送用鍵
配送用鍵を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
cccccccc 3 1998/8/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
使用する配送用鍵

【図７】


EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
配送用鍵を送信
使用する配送用鍵
コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
使用する配送用鍵
を配送信用鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵

【図８】



配送用鍵	配送用鍵のバージョン	使用可能期間 開始	使用可能期間 終了
aaaaaaaaa	1	1998／1／1	1998／1／31

仮配送用鍵 Kd

【図９】

SAMのID		SAM62のID	SAM212のID
機器番号		レシーバ51の機器番号(100番)	レシーバ)201の機器番号(100番)
決済ID		ユーザFの決済ID	ユーザAの決済ID
決済ユーザ情報	氏名	ユーザFの氏名	ユーザAの氏名
	住所	ユーザFの住所	ユーザAの住所
	電話番号	ユーザFの電話番号	ユーザAの電話番号
	決済機関情報	ユーザFの決済情報	ユーザAの決済情報
	生年月日	ユーザFの生年月日	ユーザAの生年月日
	年齢	ユーザFの年齢	ユーザAの年齢
	性別	ユーザFの性別(男)	ユーザAの性別(女)
	ユーザのID	ユーザFのID	ユーザAのID
	パスワード	ユーザFのパスワード	ユーザAのパスワード
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ポイント情報		レシーバ51の利用ポイント情報	レシーバ201利用ポイント情報

システム登録情報

【図１０】

(A)

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

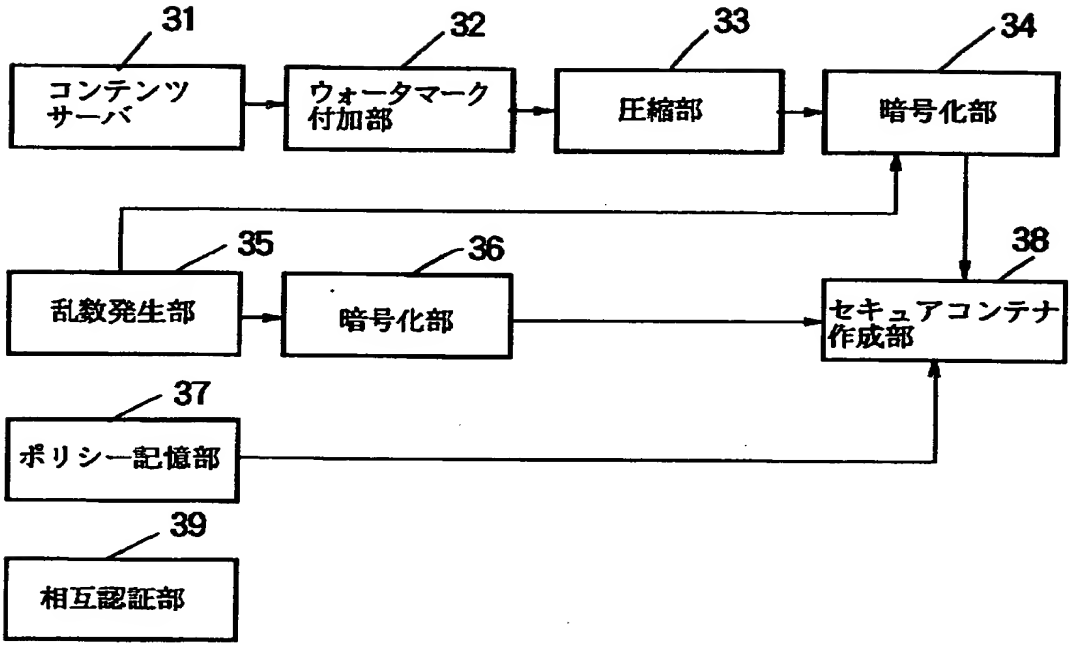
利用ポイント情報

(B)

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

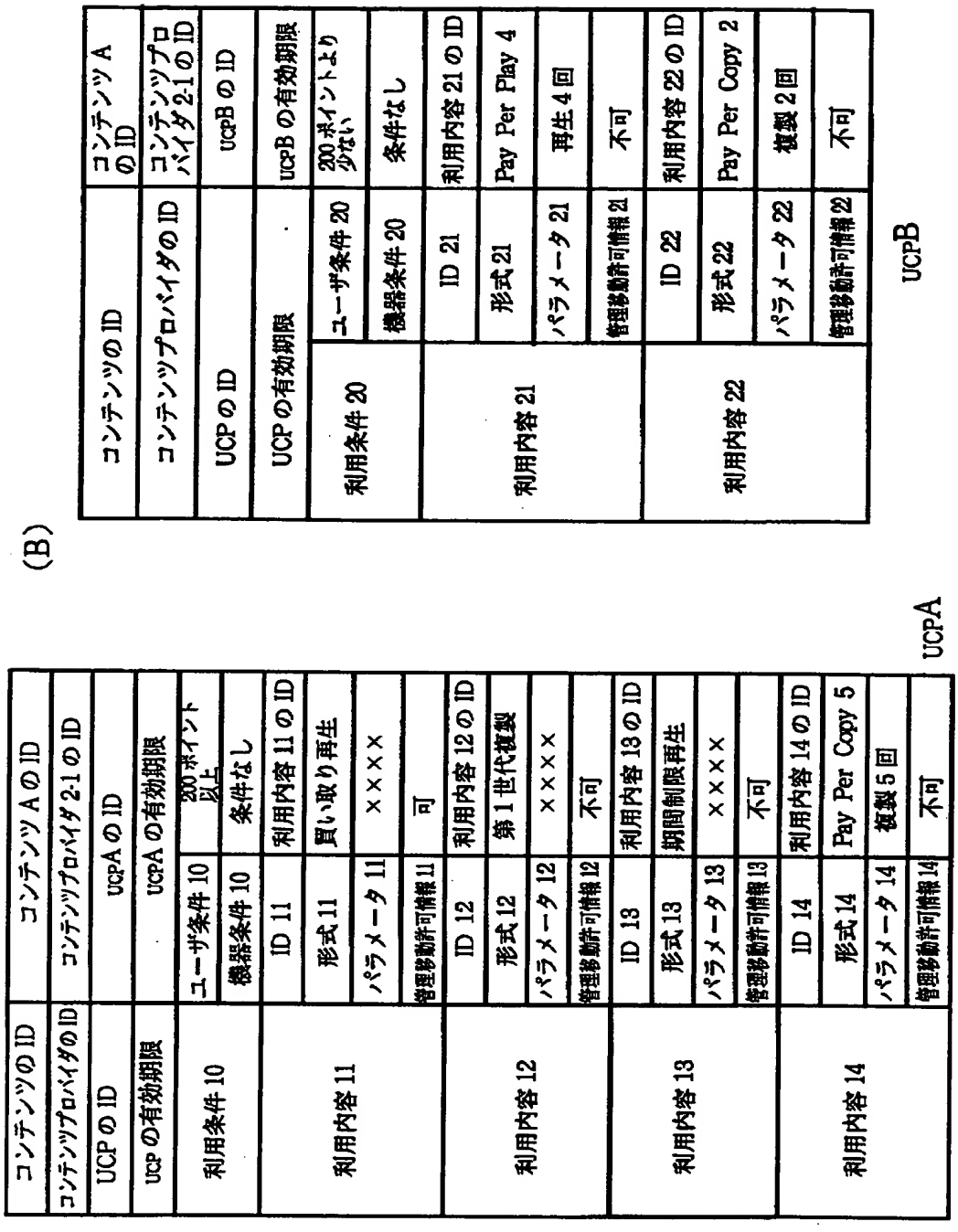
利用ポイント情報

【図１１】

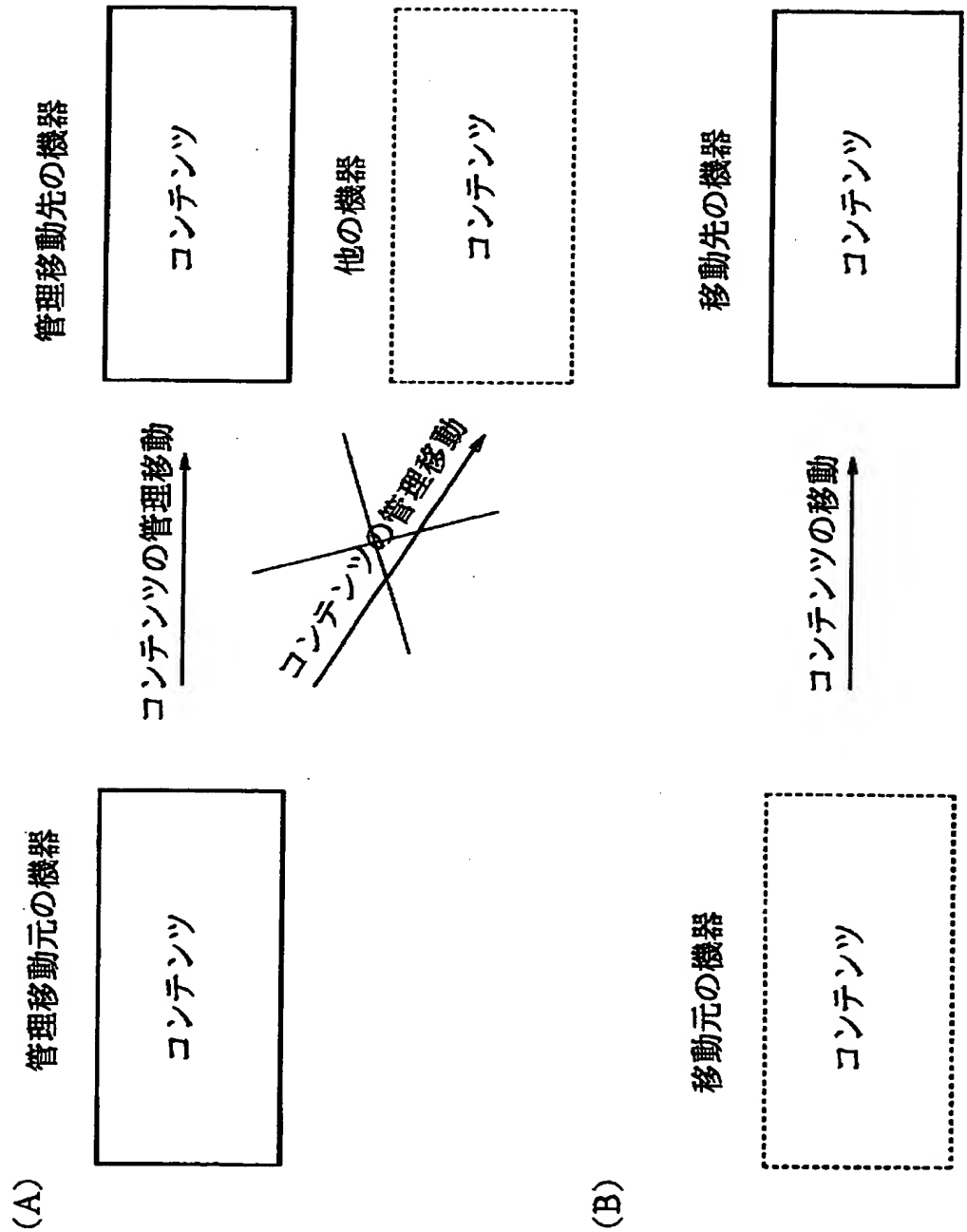


コンテンツプロバイダ 2-1

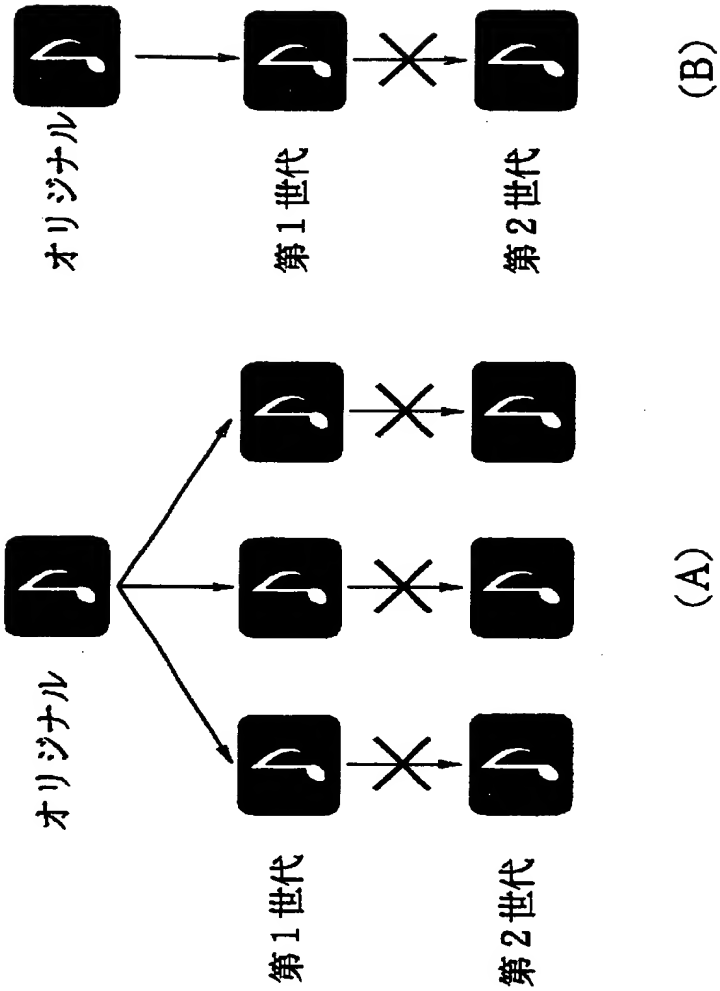
【図１２】


(A)
コンテンツのID
コンテンツプロバイダのID
UCPのID
UCPの有効期限
利用条件10
ユーザ条件10
機器条件10
利用内容11
ID11
形式11
パラメータ11
管理移動許可情報11
利用内容12
ID12
形式12
パラメータ12
管理移動許可情報12
利用内容13
ID13
形式13
パラメータ13
管理移動許可情報13
利用内容14
ID14
形式14
パラメータ14
管理移動許可情報14
コンテンツAのID
コンテンツプロバイダ2-1のID
UCPAのID
UCPAの有効期限
200ポイント以上
条件なし
利用内容11のID
買い取り再生
××××
可
利用内容12のID
第1世代複製
××××
不可
利用内容13のID
期間制限再生
××××
不可
利用内容14のID
Pay Per Copy 5
複製5回
不可
UCPA
(B)
コンテンツのID
コンテンツプロバイダのID
UCPのID
UCPの有効期限
利用条件20
ユーザ条件20
機器条件20
利用内容21
ID21
形式21
パラメータ21
管理移動許可情報21
利用内容22
ID22
形式22
パラメータ22
管理移動許可情報22
コンテンツAのID
コンテンツプロバイダ2-1のID
UCPBのID
UCPBの有効期限
200ポイントより少ない
条件なし
利用内容21のID
Pay Per Play 4
再生4回
不可
利用内容22のID
Pay Per Copy 2
複製2回
不可
UCPB

【図１３】


(A)
管理移動元の機器
コンテンツ
コンテンツの管理移動
管理移動先の機器
コンテンツ
他の機器
コンテンツ
コンテンツの管理移動
(B)
移動元の機器
コンテンツ
コンテンツの移動
移動先の機器
コンテンツ

【図１４】



【図１５】

（A）

サービスコード	意　味
0000h	条件なし
0001h 乃至 00FFh	機器に関し条件有り
0100h 乃至 01FFh	性別条件あり
0200h 乃至 02FFh	年令条件あり
0300h 乃至 7FFFh	その他の条件あり
8000h 乃至 FFFFh	利用ポイントに関し条件有り

（B）

コンディションコード	意　味
00h	無条件
01h	＝
02h	≠
03h	＜（より小さい）
04h	＞（より大きい）
05h	≦（以下）
06h	≧（以上）
07h 乃至 FFh	空き

【図１６】

（A）

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	80××h	0000C8h	06h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

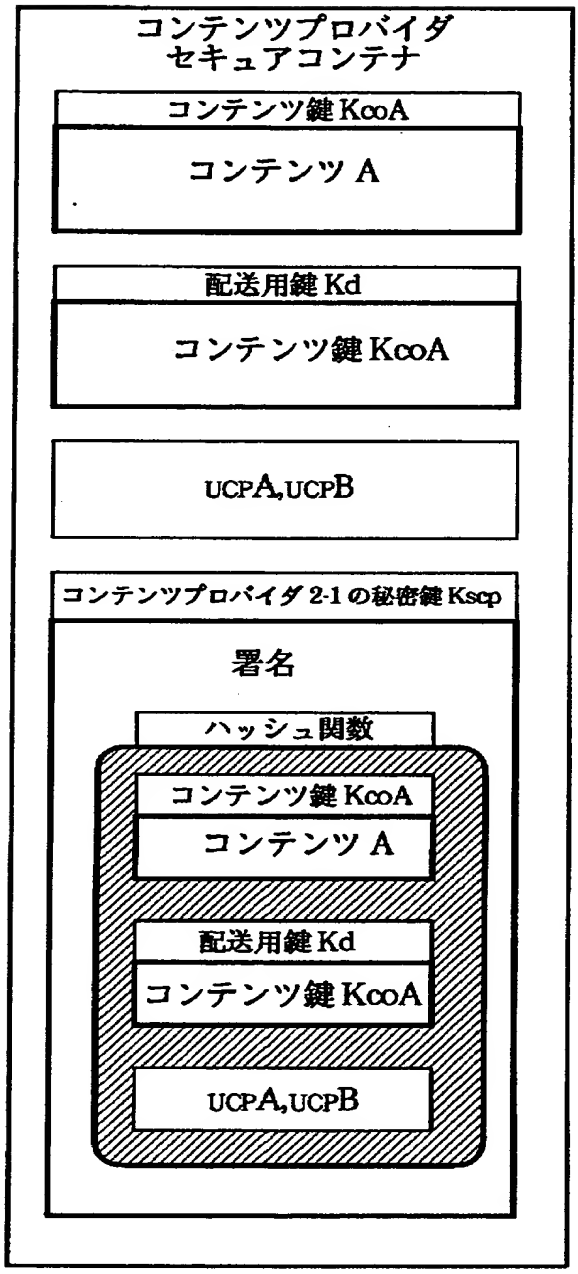
UCPA の利用条件 10

（B）

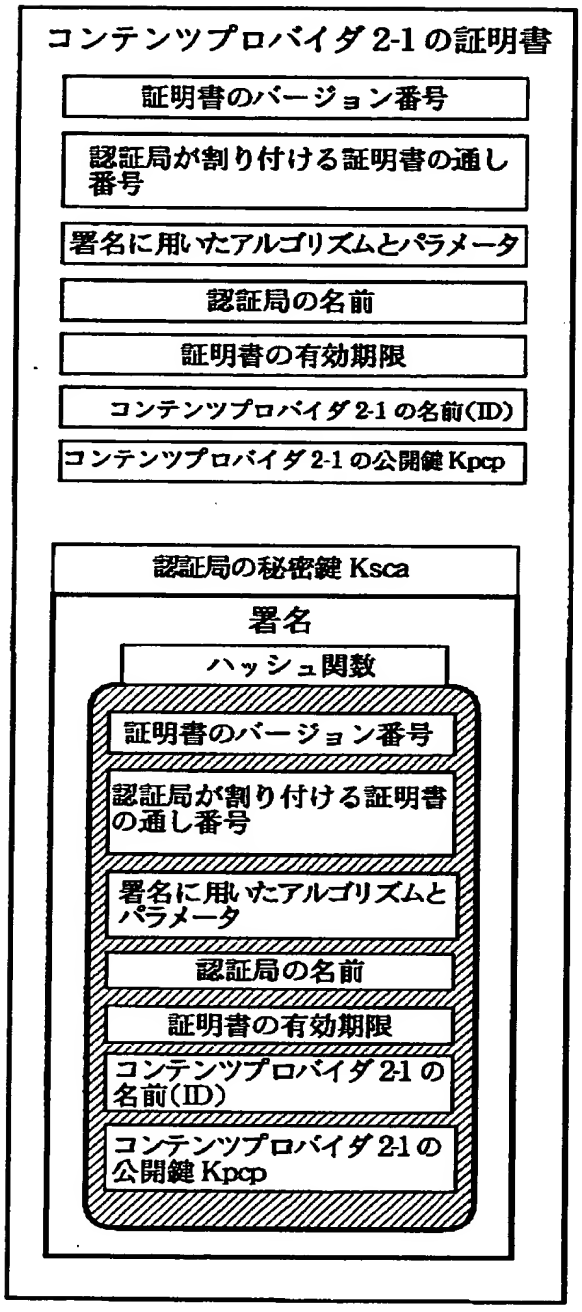
ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	80××h	0000C8h	03h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPB の利用条件 20

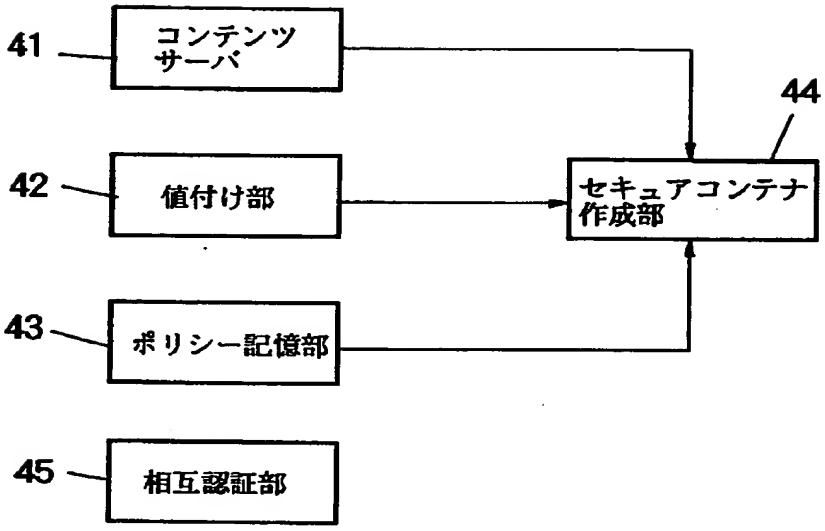
【図１７】


コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵 KcoA
コンテンツ A
配送用鍵 Kd
コンテンツ鍵 KcoA
UCPA,UCPB
コンテンツプロバイダ 2-1 の秘密鍵 Kscp
署名
ハッシュ関数
コンテンツ鍵 KcoA
コンテンツ A
配送用鍵 Kd
コンテンツ鍵 KcoA
UCPA,UCPB

【図１８】


コンテンツプロバイダ2-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダ2-1の名前(ID)
コンテンツプロバイダ2-1の公開鍵Kpcp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
コンテンツプロバイダ2-1の名前(ID)
コンテンツプロバイダ2-1の公開鍵Kpcp

【図１９】


41
コンテンツサーバ
42
値付け部
43
ポリシー記憶部
45
相互認証部
44
セキュアコンテナ作成部
サービスプロバイダ 3-1

【図２０】

(A)

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2-1のID		
UCPのID	UCPAのID		
サービスプロバイダのID	サービスプロバイダ3-1のID		
PTのID	PTA-1のID		
PTの有効期限	PTA-1の有効期限		
価格条件10	ユーザ条件10	男性	
	機器条件10	条件なし	
価格内容11	2000円		
価格内容12	600円		
価格内容13	100円		
価格内容14	300円		

PTA-1

(B)

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2-1のID		
UCPのID	UCPAのID		
サービスプロバイダのID	サービスプロバイダ3-1のID		
PTのID	PTA-2のID		
PTの有効期限	PTA-2の有効期限		
価格条件20	ユーザ条件20	女性	
	機器条件20	条件なし	
価格内容21	1000円		
価格内容22	800円		
価格内容23	50円		
価格内容24	150円		

PTA-2

【図２１】

（A）

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1 の価格条件 10

（B）

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	01××h	000001h	01h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2 の価格条件 20

【図２２】

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2-1のID		
UCPのID	UCPBのID		
サービスプロバイダのID	サービスプロバイダ3-1のID		
PTのID	PTB-1のID		
PTの有効期限	PTB-1の有効期限		
価格条件30	ユーザ条件30	条件なし	
	機器条件30	従機器	
価格内容31	100円		
価格内容32	300円		

PTB-1

(A)

コンテンツのID	コンテンツAのID		
コンテンツプロバイダのID	コンテンツプロバイダ2-1のID		
UCPのID	UCPBのID		
サービスプロバイダのID	サービスプロバイダ3-1のID		
PTのID	PTB-2のID		
PTの有効期限	PTB-2の有効期限		
価格条件40	ユーザ条件40	条件なし	
	機器条件40	主機器	
価格内容41	50円		
価格内容42	150円		

PTB-2

(B)

【図２３】

(A)

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00××h	000064h	03h

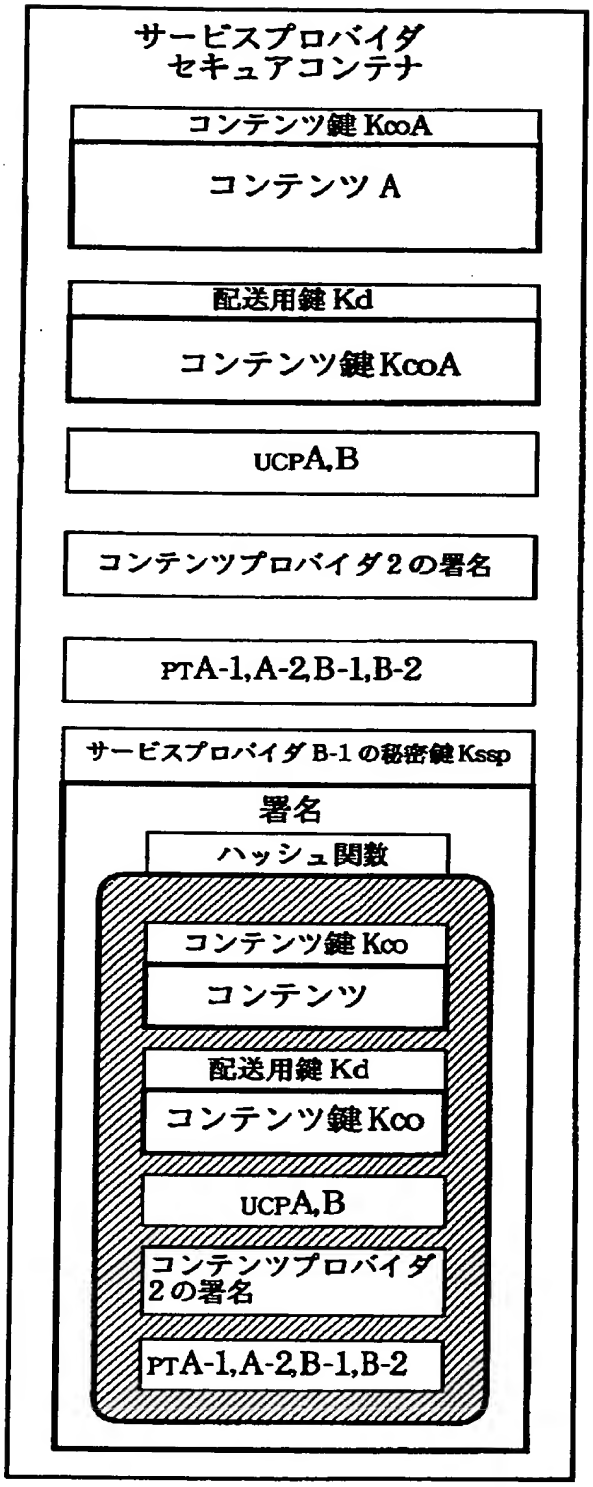
PTB-1 の価格条件 30

(B)

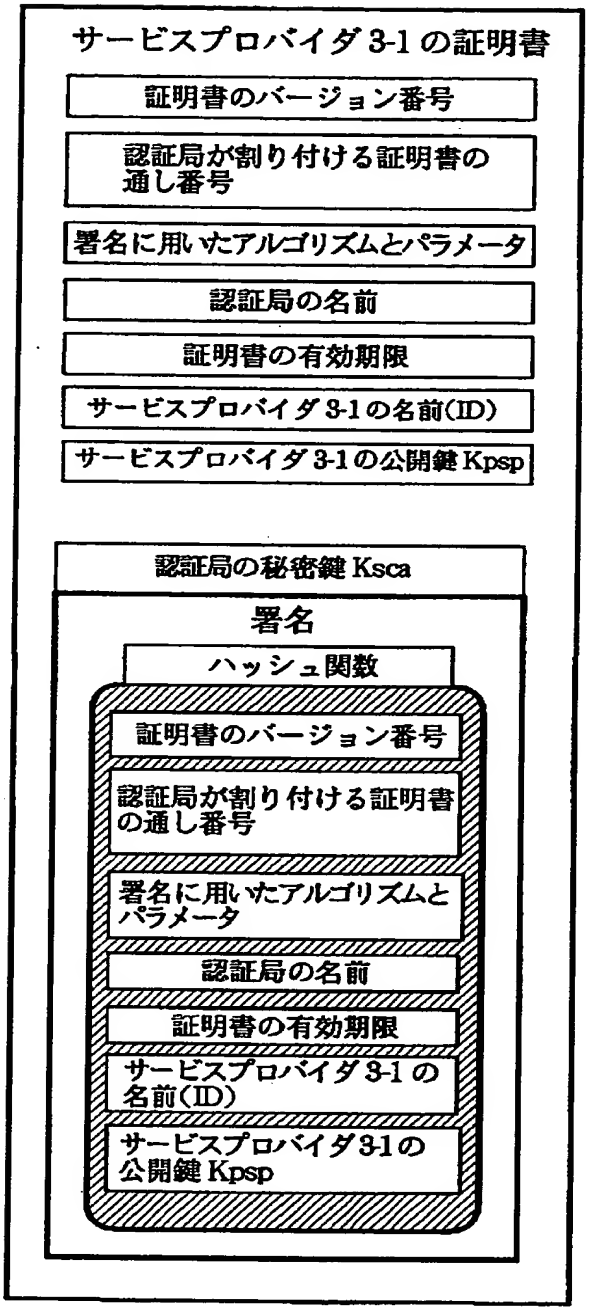
ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00××h	000064h	06h

PTB-2 の価格条件 40

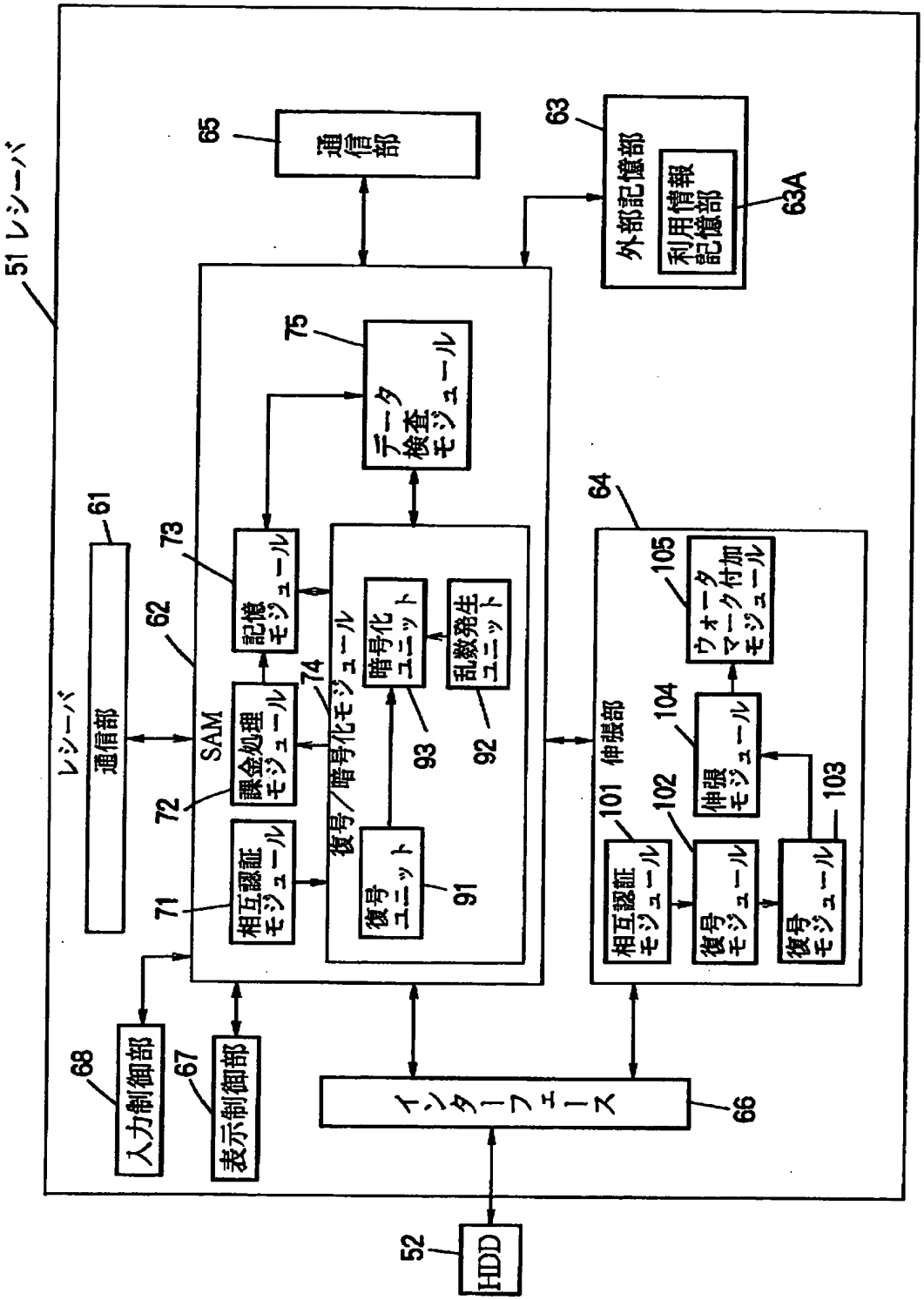
【図２４】


サービスプロバイダ
セキュアコンテナ
コンテンツ鍵 KcoA
コンテンツ A
配送用鍵 Kd
コンテンツ鍵 KcoA
UCPA,B
コンテンツプロバイダ２の署名
PTA-1,A-2,B-1,B-2
サービスプロバイダ B-1 の秘密鍵 Kssp
署名
ハッシュ関数
コンテンツ鍵 Kco
コンテンツ
配送用鍵 Kd
コンテンツ鍵 Kco
UCPA,B
コンテンツプロバイダ２の署名
PTA-1,A-2,B-1,B-2

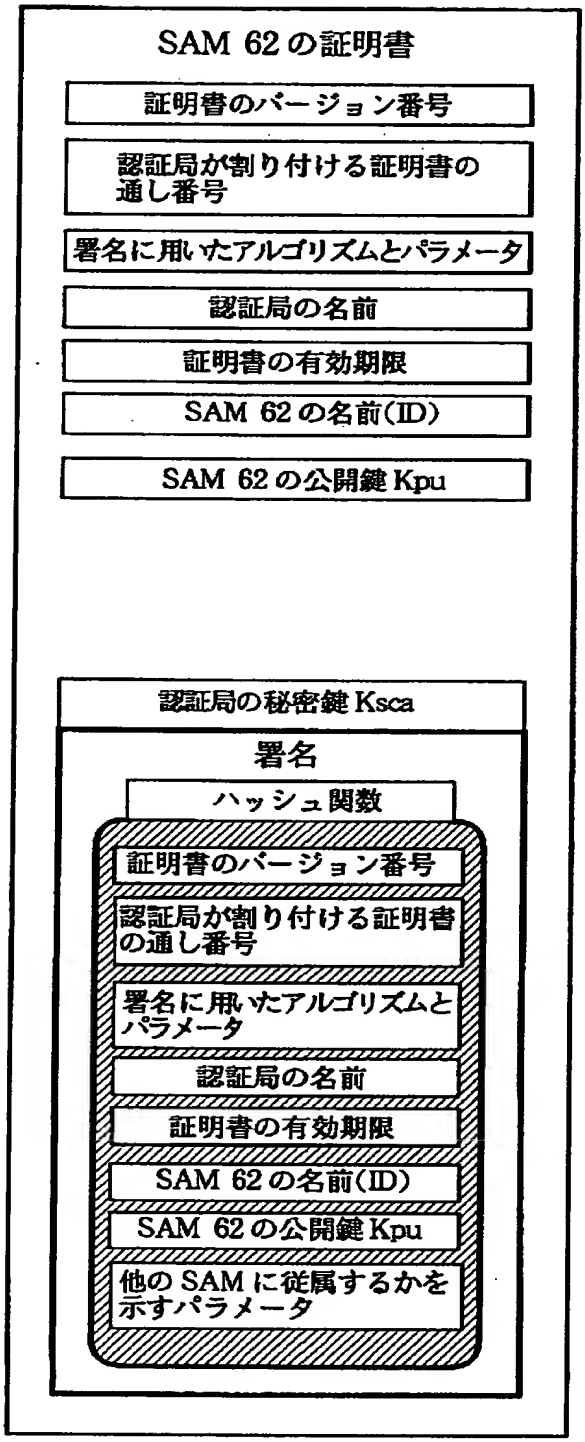
【図２５】


サービスプロバイダ3-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダ3-1の名前(ID)
サービスプロバイダ3-1の公開鍵Kpsp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
サービスプロバイダ3-1の名前(ID)
サービスプロバイダ3-1の公開鍵Kpsp

【図２６】


51 レシーバ
65 通信部
63 外部記憶部
利用情報記憶部
63A
75 データ検査モジュール
64
61
73 記憶モジュール
62
105 ウォータマーク付加モジュール
レシーバ通信部
SAM
74 暗号化モジュール
暗号化ユニット
乱数発生ユニット
93
92
104 伸張モジュール
103
72 課金処理モジュール
復号／暗号化モジュール
101 伸張部
102
71 相互認証モジュール
復号ユニット
91
相互認証モジュール
復号モジュール
復号モジュール
68 入力制御部
67 表示制御部
インターフェース
66
52 HDD

【図２７】

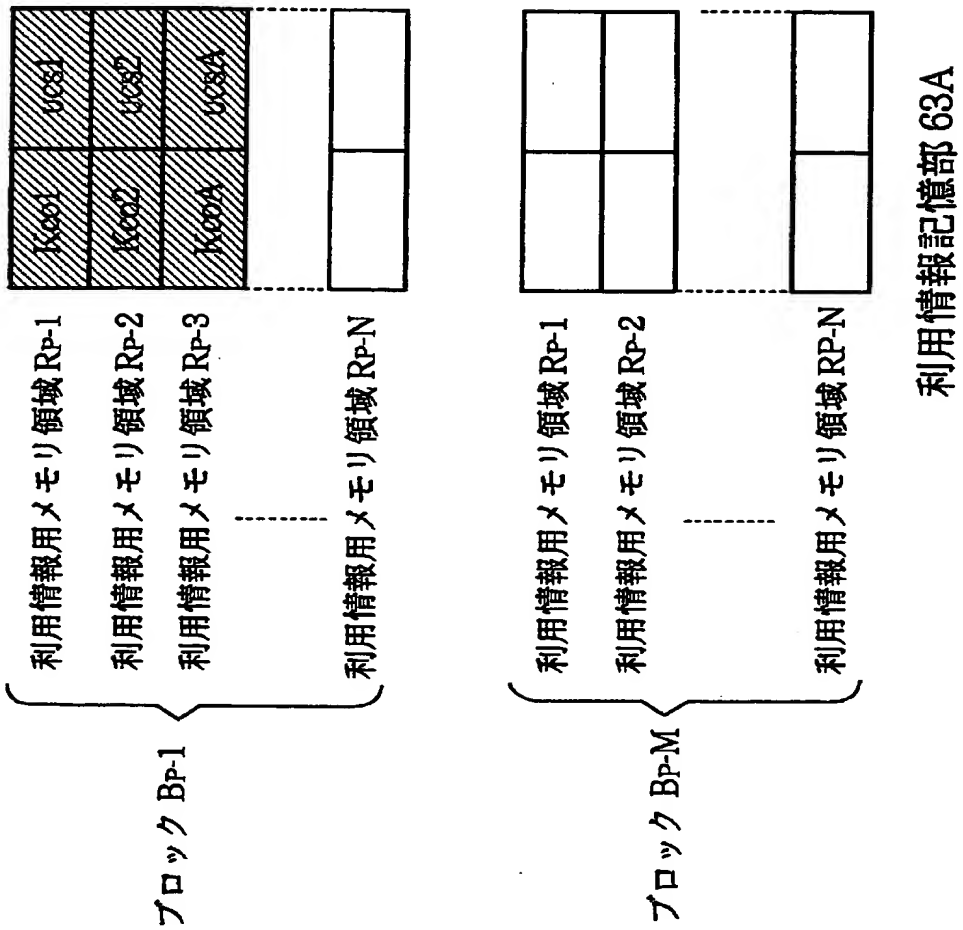

SAM 62の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
他のSAMに従属するかを示すパラメータ

【図２８】

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元：SAM62のID、管理移動先：SAM62のID
利用履歴		×××

UCSA

【図２９】

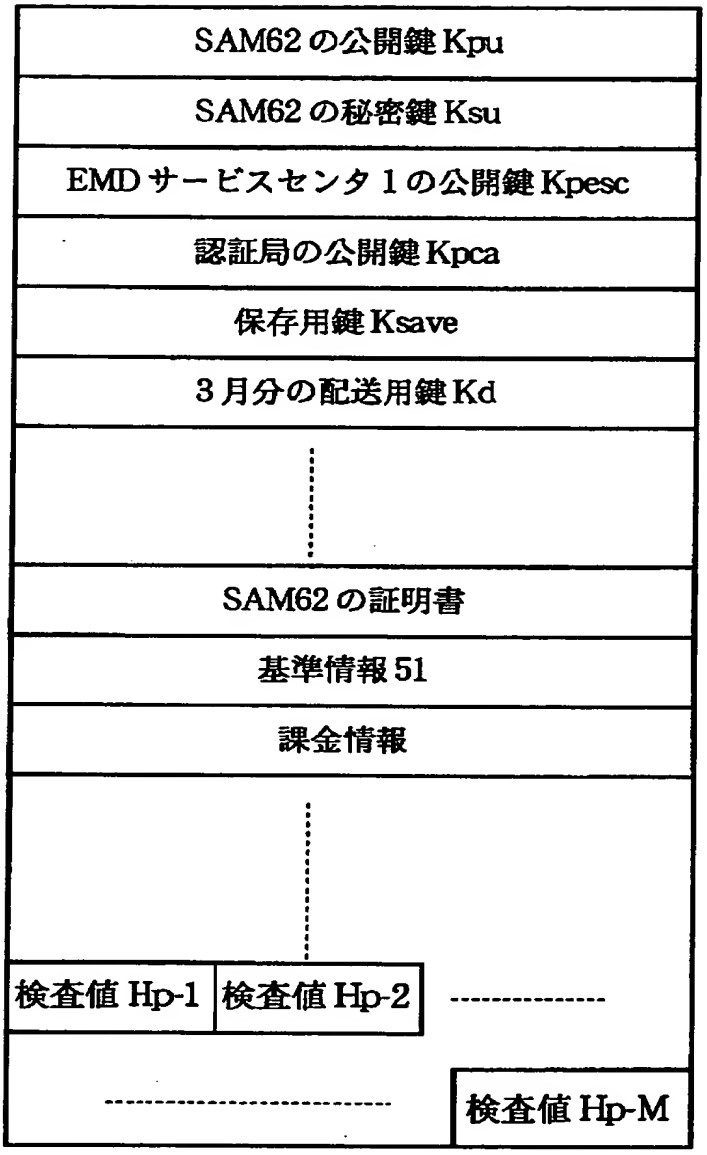

利用情報用メモリ領域 RP-1
利用情報用メモリ領域 RP-2
利用情報用メモリ領域 RP-3
利用情報用メモリ領域 RP-N
KCB1
KCB2
KCB3A
ブロック BP-1
利用情報用メモリ領域 RP-1
利用情報用メモリ領域 RP-2
利用情報用メモリ領域 RP-N
ブロック BP-M
利用情報記憶部 63A

【図３０】

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元：SAM62のID、管理移動先：SAM62のID
課金履歴		×××

課金情報A

【図３１】


SAM62の公開鍵Kpu
SAM62の秘密鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM62の証明書
基準情報51
課金情報
検査値Hp-1
検査値Hp-2
検査値Hp-M

【図３２】

SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号（100 番）
決済 ID		ユーザＦの決済 ID
課金の上限額		正式登録時の課金の上限額
決済ユーザ情報	氏名	ユーザＦの氏名
	住所	ユーザＦの住所
	電話番号	ユーザＦの電話番号
	決済機関情報	ユーザＦの決済機関情報
	生年月日	ユーザＦの生年月日
	年齢	ユーザＦの年齢（21 才）
	性別	ユーザＦの性別（男）
	ユーザの ID	ユーザＦの ID
	パスワード	ユーザＦのパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
利用ポイント情報		レシーバ 51 の利用ポイント情報

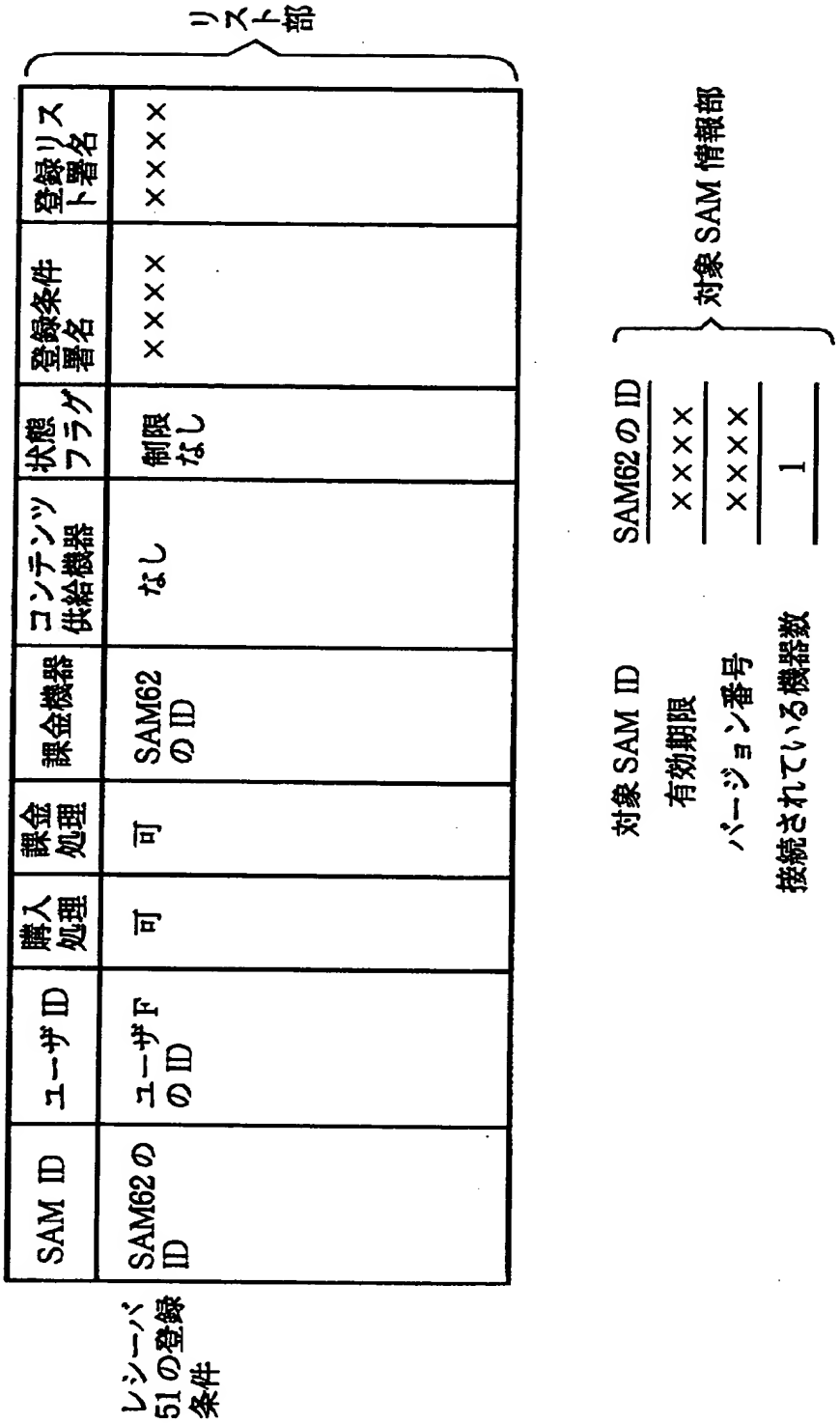
基準情報 51

【図３３】

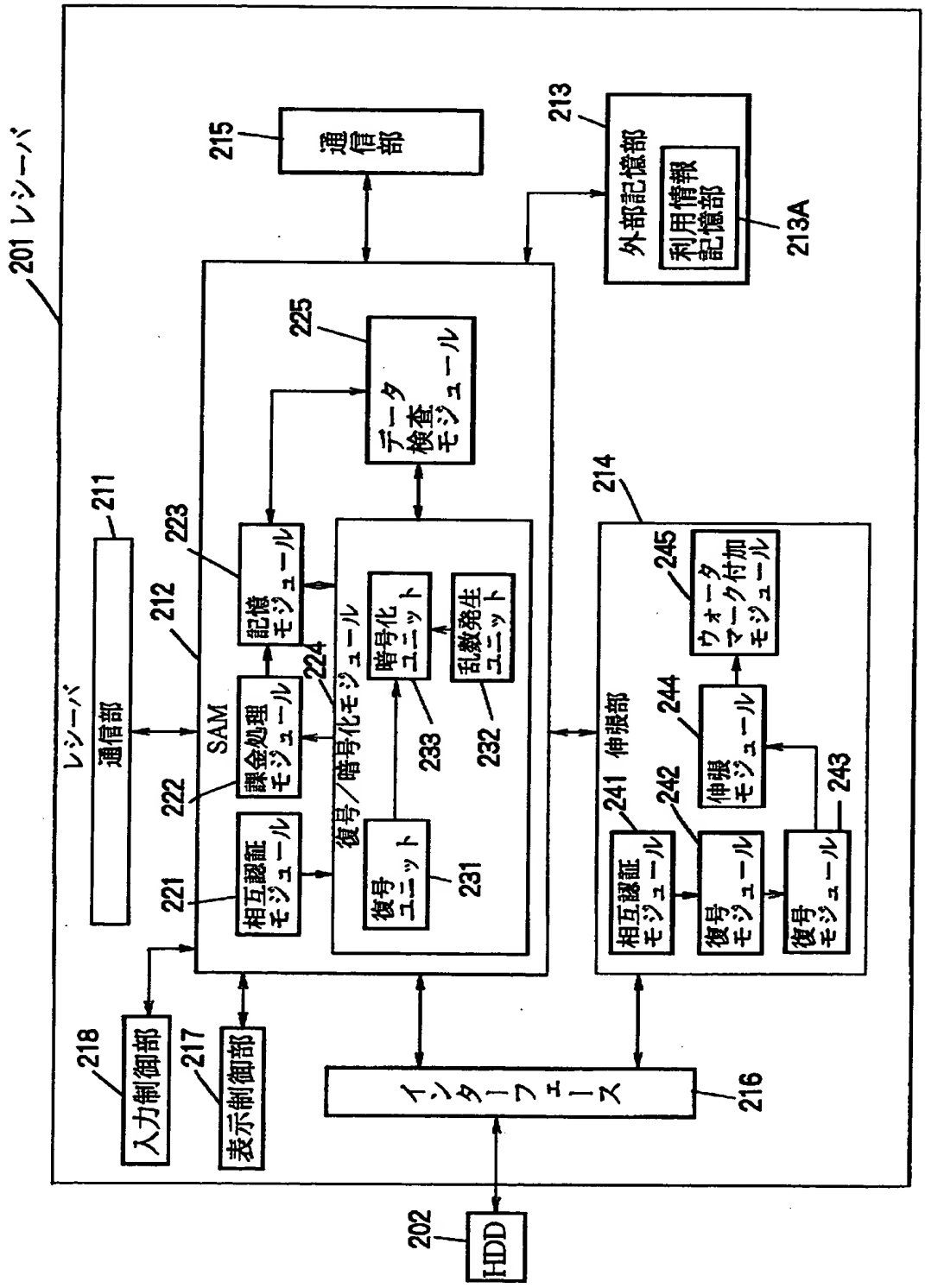
ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

基準情報51の利用ポイント情報

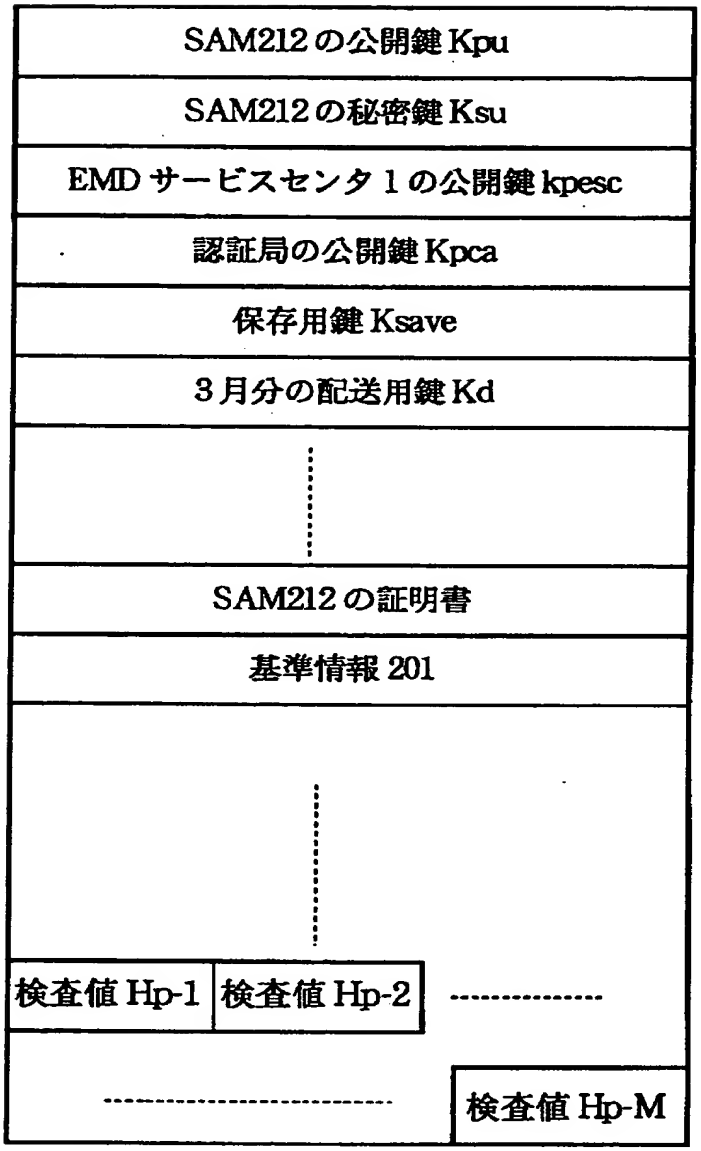
【図３４】


リスト部
SAM ID
ユーザ ID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
SAM62のID
ユーザFのID
可
可
SAM62のID
なし
制限なし
××××
××××
レシーバ51の登録条件
対象 SAM 情報部
対象 SAM ID
SAM62 の ID
有効期限
××××
バージョン番号
××××
接続されている機器数
1

【図３５】


201 レシーバ
215
通信部
213
外部記憶部
利用情報記憶部
213A
225
データ検査モジュール
214
211
223
記憶モジュール
212
SAM
224
課金処理モジュール
222
相互認証モジュール
221
復号／暗号化モジュール
暗号化ユニット
乱数発生ユニット
233
232
復号ユニット
231
伸張部
245
ウォータマーク付加モジュール
244
伸張モジュール
241
242
243
相互認証モジュール
復号モジュール
復号モジュール
レシーバ
通信部
218
入力制御部
217
表示制御部
インターフェース
216
202
HDD

【図３６】


SAM212の公開鍵Kpu
SAM212の秘密鍵Ksu
EMDサービスセンタ1の公開鍵kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM212の証明書
基準情報201
検査値Hp-1
検査値Hp-2
検査値Hp-M

【図３７】

SAM の ID		SAM62 の ID
機器番号		レシーバ 201 の機器番号（100 番）
決済 ID		ユーザ A の決済 ID
課金の上限額		正式登録時の上限額
決済ユーザ情報	氏名	ユーザ A の氏名
	住所	ユーザ A の住所
	電話番号	ユーザ A の電話番号
	決済機関情報	ユーザ A の決済機関情報
	生年月日	ユーザ A の生年月日
	年齢	ユーザ A の年齢
	性別	ユーザ A の性別
	ユーザの ID	ユーザ A の ID
	パスワード	ユーザ A のパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
利用ポイント情報		レシーバ 201 の利用ポイント情報

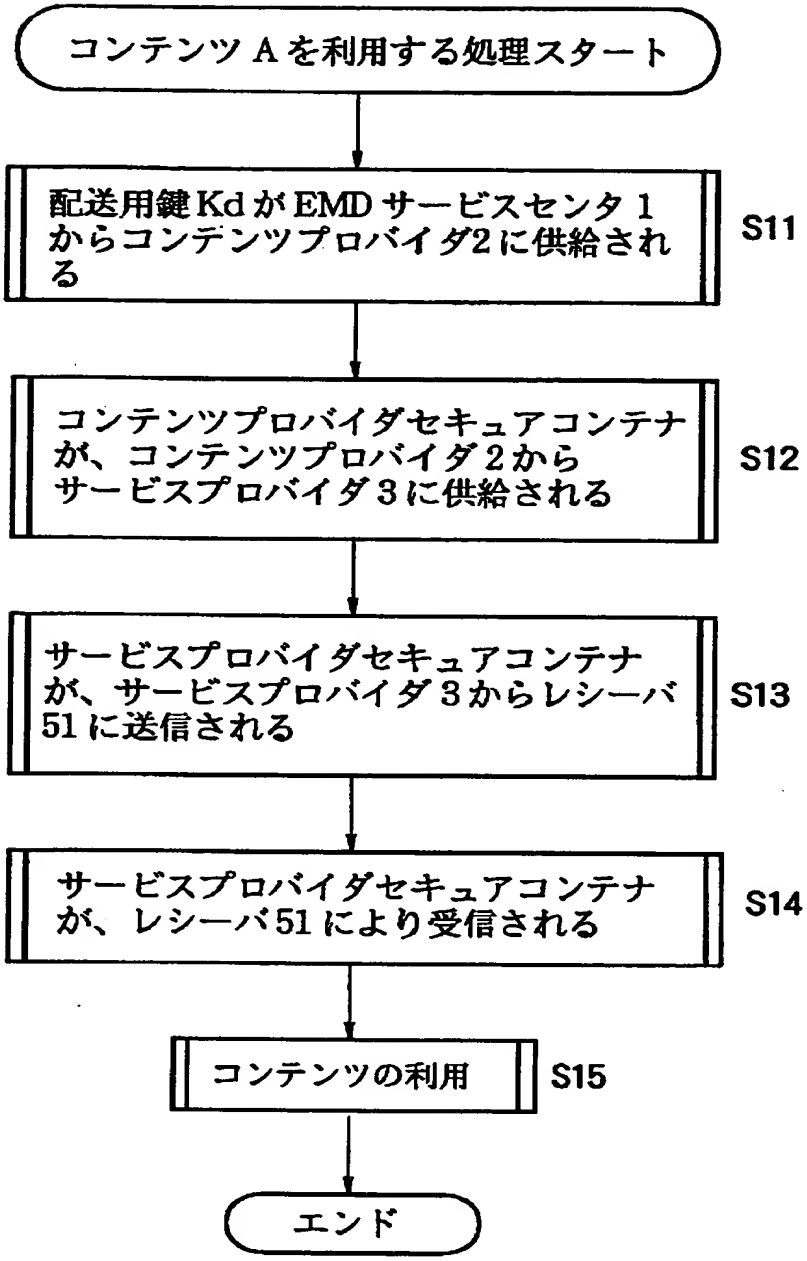
基準情報 201

【図３８】

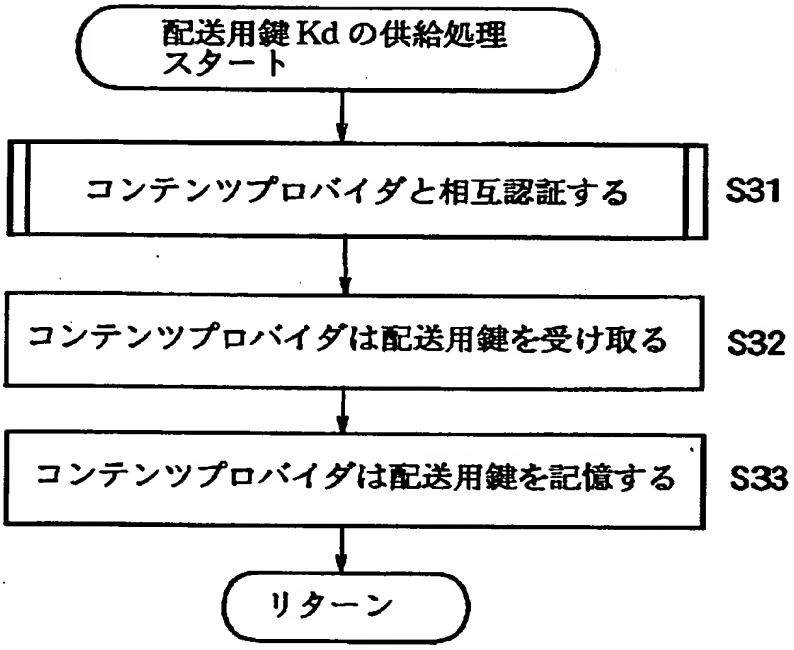
ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

基準情報201の利用ポイント情報

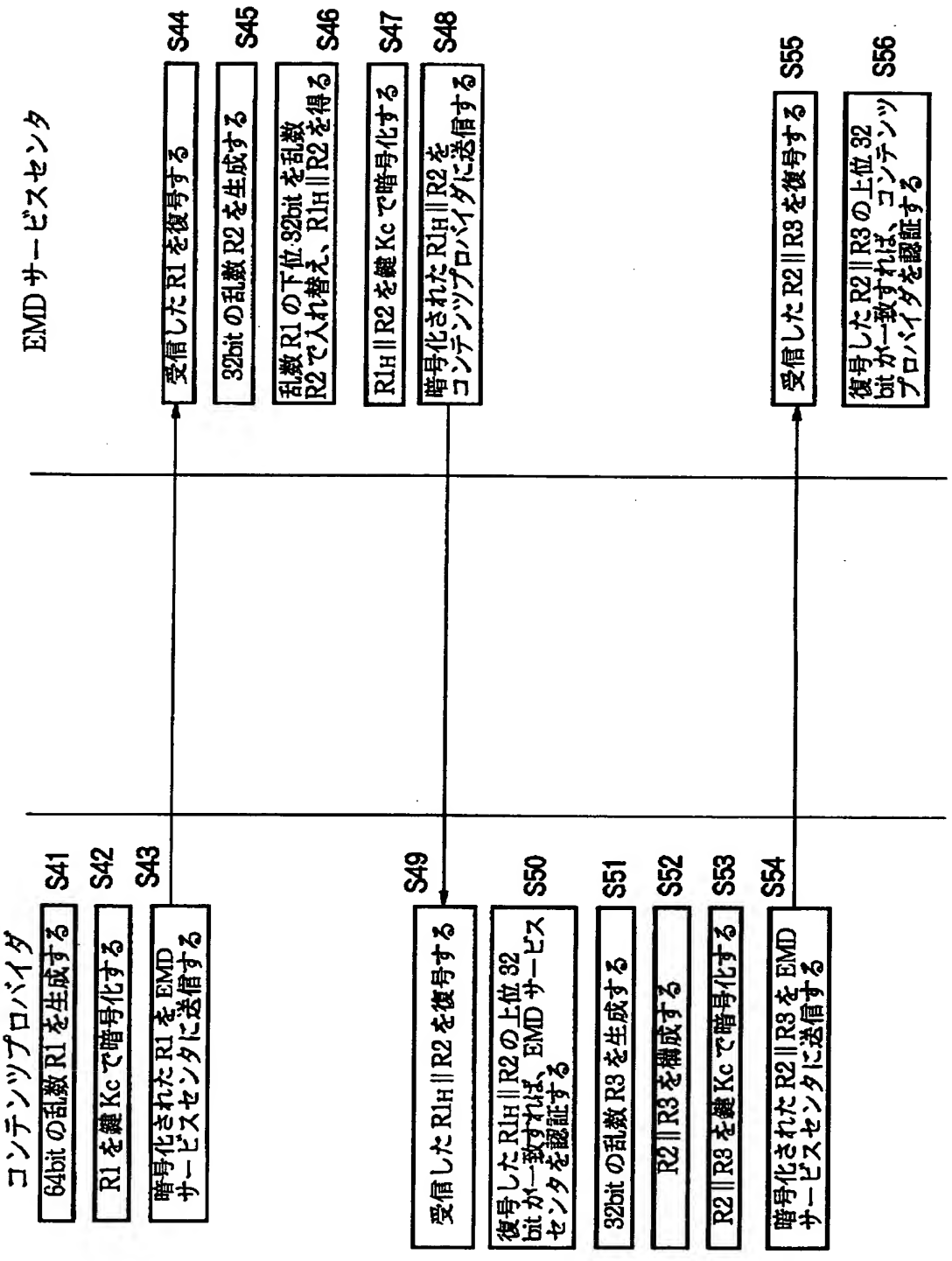
【図３９】


コンテンツＡを利用する処理スタート
配送用鍵KdがEMDサービスセンタ1からコンテンツプロバイダ2に供給される
S11
コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2からサービスプロバイダ3に供給される
S12
サービスプロバイダセキュアコンテナが、サービスプロバイダ3からレシーバ51に送信される
S13
サービスプロバイダセキュアコンテナが、レシーバ51により受信される
S14
コンテンツの利用
S15
エンド

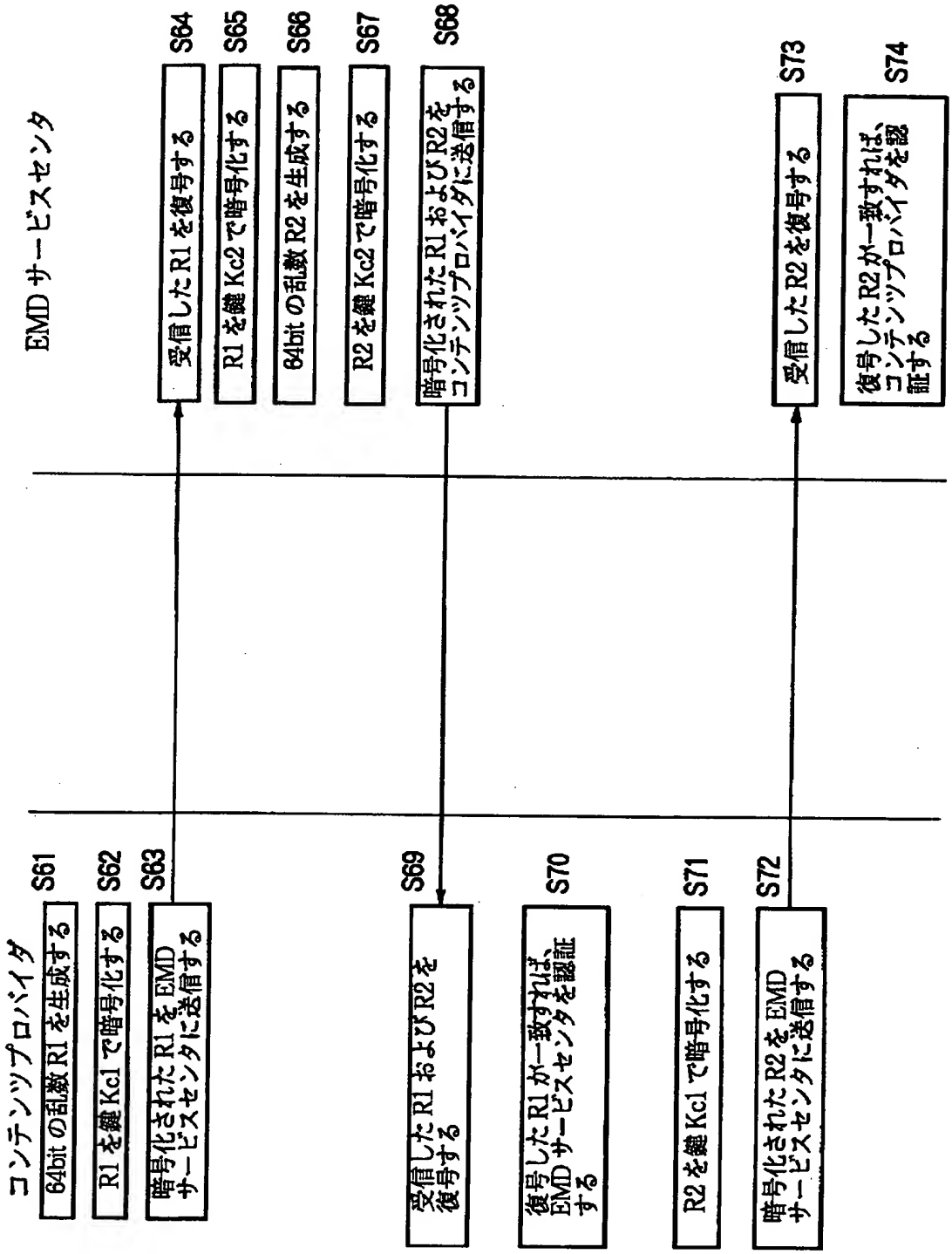
【図４０】


配送用鍵Kdの供給処理
スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

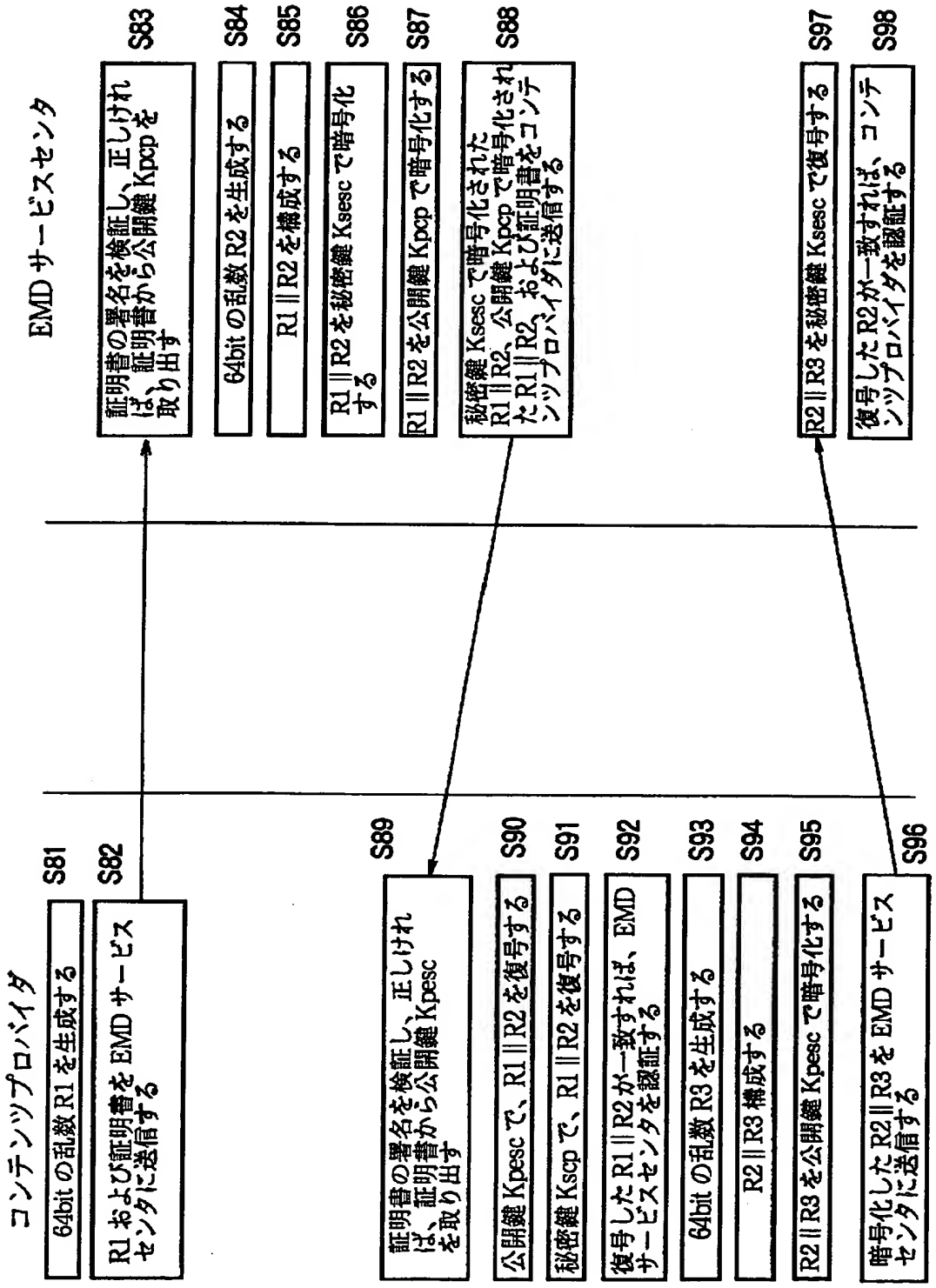
【図４１】


コンテンツプロバイダ
EMDサービスセンタ
S41
64bitの乱数R1を生成する
S42
R1を鍵Kcで暗号化する
S43
暗号化されたR1をEMDサービスセンタに送信する
S44
受信したR1を復号する
S45
32bitの乱数R2を生成する
S46
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S47
R1H||R2を鍵Kcで暗号化する
S48
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S49
受信したR1H||R2を復号する
S50
復号したR1H||R2の上位32bitが一致すれば、EMDサービスセンタを認証する
S51
32bitの乱数R3を生成する
S52
R2||R3を構成する
S53
R2||R3を鍵Kcで暗号化する
S54
暗号化されたR2||R3をEMDサービスセンタに送信する
S55
受信したR2||R3を復号する
S56
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する

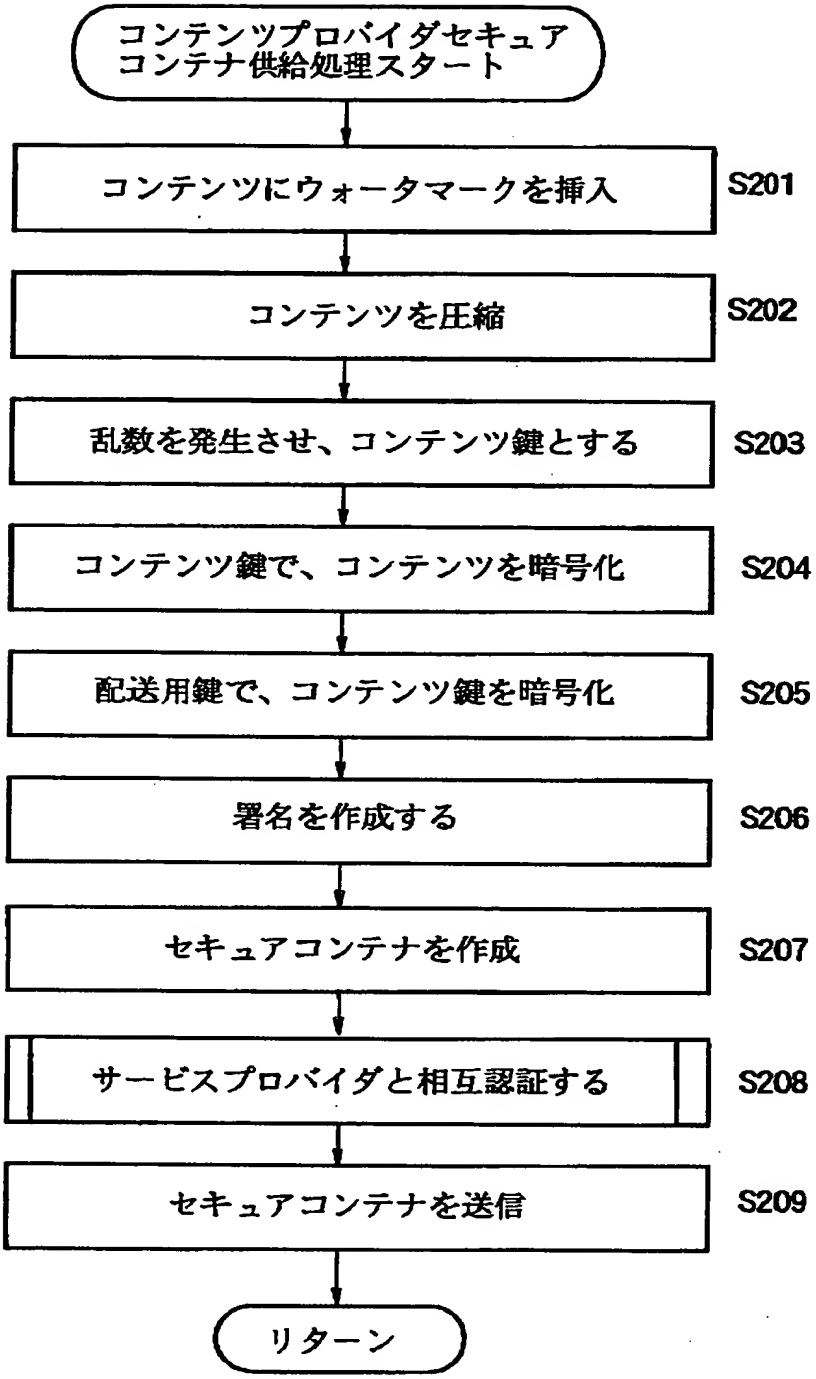
【図４２】


コンテンツプロバイダ
EMDサービスセンタ
S61
64bitの乱数R1を生成する
S62
R1を鍵Kc1で暗号化する
S63
暗号化されたR1をEMDサービスセンタに送信する
S64
受信したR1を復号する
S65
R1を鍵Kc2で暗号化する
S66
64bitの乱数R2を生成する
S67
R2を鍵Kc2で暗号化する
S68
暗号化されたR1およびR2をコンテンツプロバイダに送信する
S69
受信したR1およびR2を復号する
S70
復号したR1が一致すれば、EMDサービスセンタを認証する
S71
R2を鍵Kc1で暗号化する
S72
暗号化されたR2をEMDサービスセンタに送信する
S73
受信したR2を復号する
S74
復号したR2が一致すれば、コンテンツプロバイダを認証する

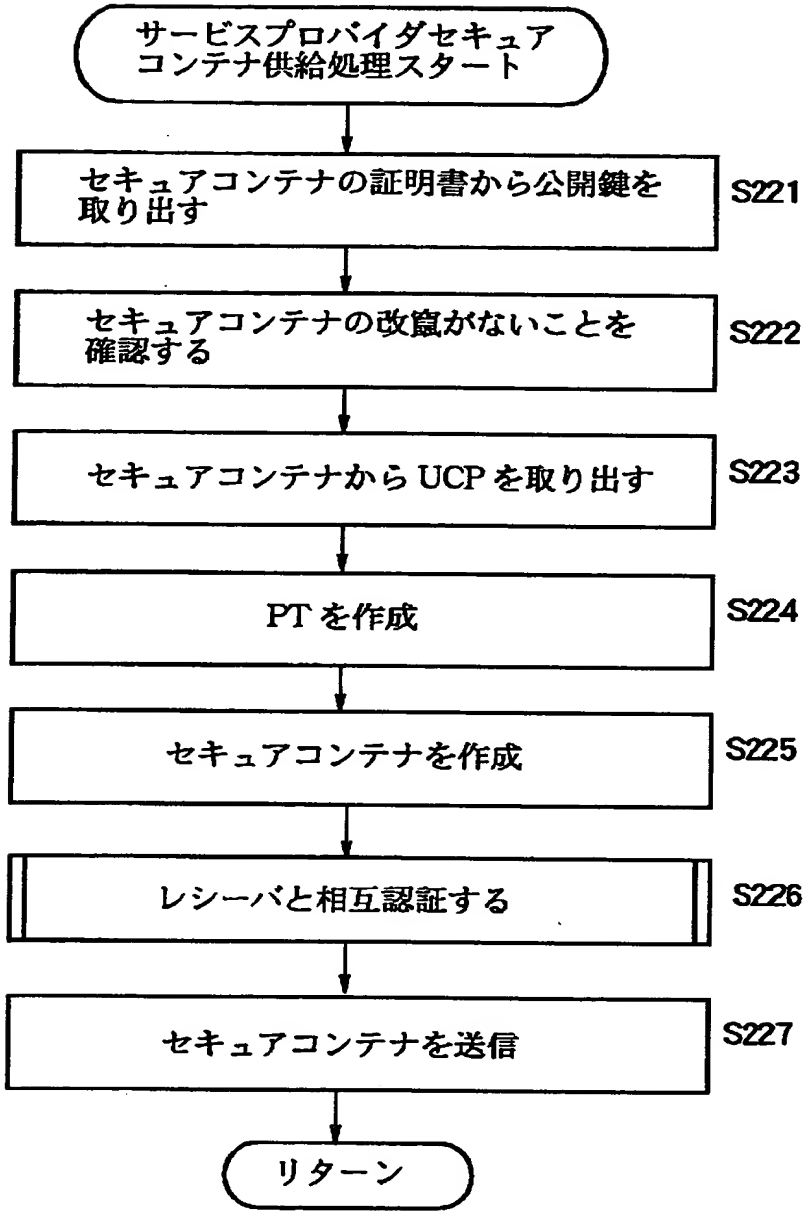
【図４３】


コンテンツプロバイダ
EMDサービスセンタ
S81
64bitの乱数R1を生成する
S82
R1および証明書をEMDサービスセンタに送信する
S83
証明書の署名を検証し、正しければ、証明書から公開鍵Kpcpを取り出す
S84
64bitの乱数R2を生成する
S85
R1||R2を構成する
S86
R1||R2を秘密鍵Ksescで暗号化する
S87
R1||R2を公開鍵Kpcpで暗号化する
S88
秘密鍵Ksescで暗号化されたR1||R2、公開鍵Kpcpで暗号化されたR1||R2、および証明書をコンテンツプロバイダに送信する
S89
証明書の署名を検証し、正しければ、証明書から公開鍵Kpescを取り出す
S90
公開鍵Kpescで、R1||R2を復号する
S91
秘密鍵Kscpで、R1||R2を復号する
S92
復号したR1||R2が一致すれば、EMDサービスセンタを認証する
S93
64bitの乱数R3を生成する
S94
R2||R3構成する
S95
R2||R3を公開鍵Kpescで暗号化する
S96
暗号化したR2||R3をEMDサービスセンタに送信する
S97
R2||R3を秘密鍵Ksescで復号する
S98
復号したR2が一致すれば、コンテンツプロバイダを認証する

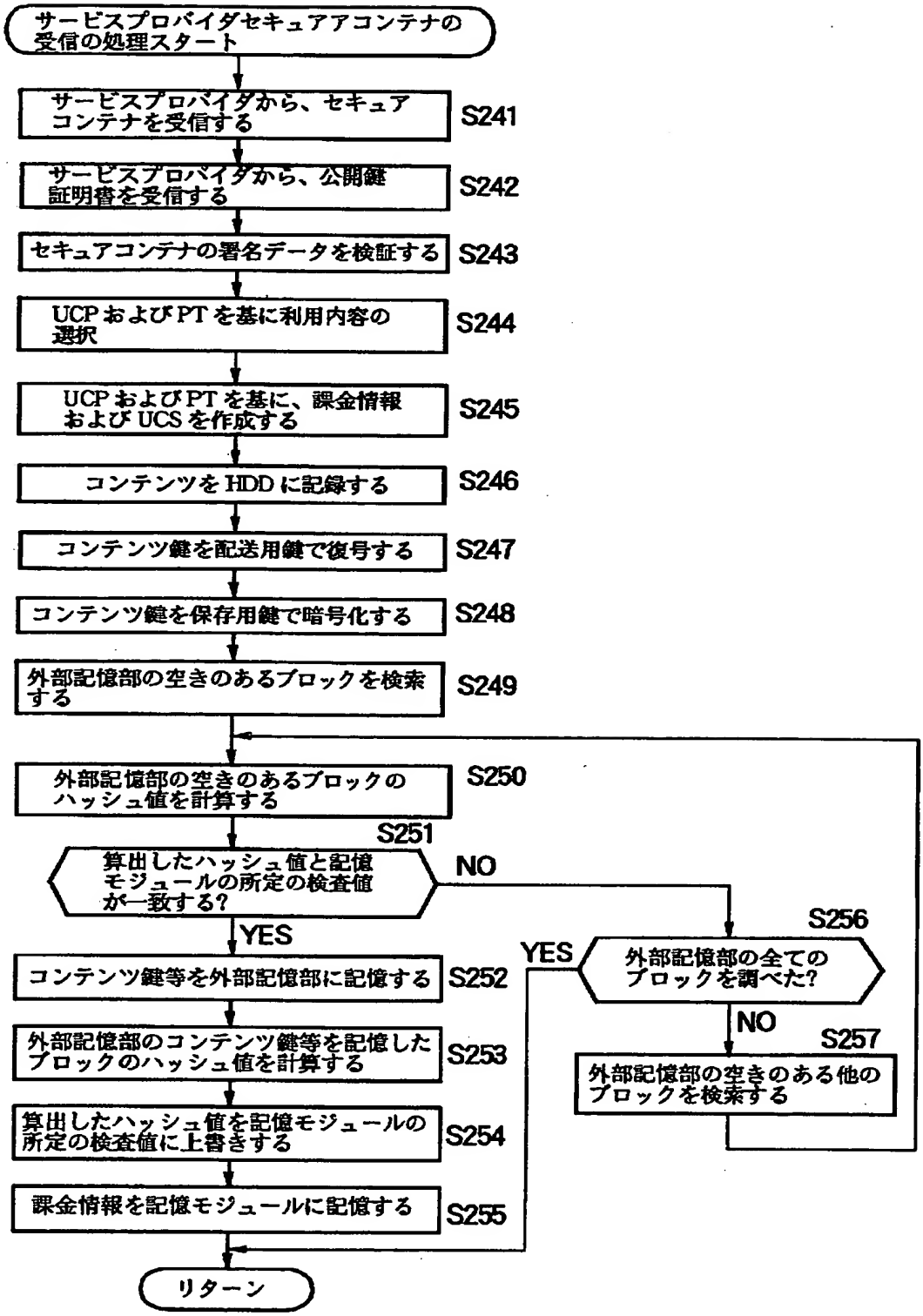
【図４４】


コンテンツプロバイダセキュア
コンテナ供給処理スタート
コンテンツにウォータマークを挿入
S201
コンテンツを圧縮
S202
乱数を発生させ、コンテンツ鍵とする
S203
コンテンツ鍵で、コンテンツを暗号化
S204
配送用鍵で、コンテンツ鍵を暗号化
S205
署名を作成する
S206
セキュアコンテナを作成
S207
サービスプロバイダと相互認証する
S208
セキュアコンテナを送信
S209
リターン

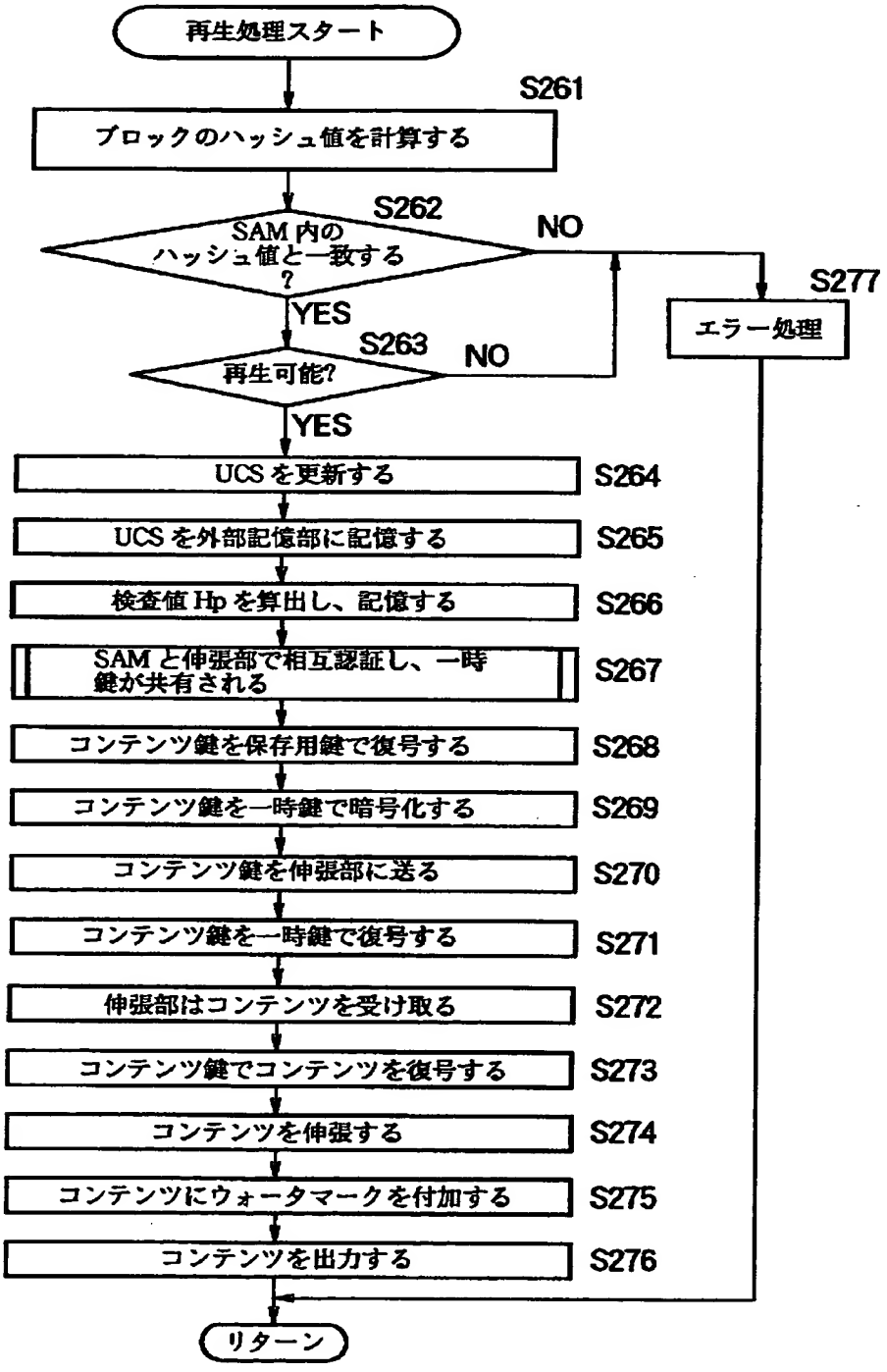
【図４５】


サービスプロバイダセキュアコンテナ供給処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S221
セキュアコンテナの改竄がないことを確認する
S222
セキュアコンテナからUCPを取り出す
S223
PTを作成
S224
セキュアコンテナを作成
S225
レシーバと相互認証する
S226
セキュアコンテナを送信
S227
リターン

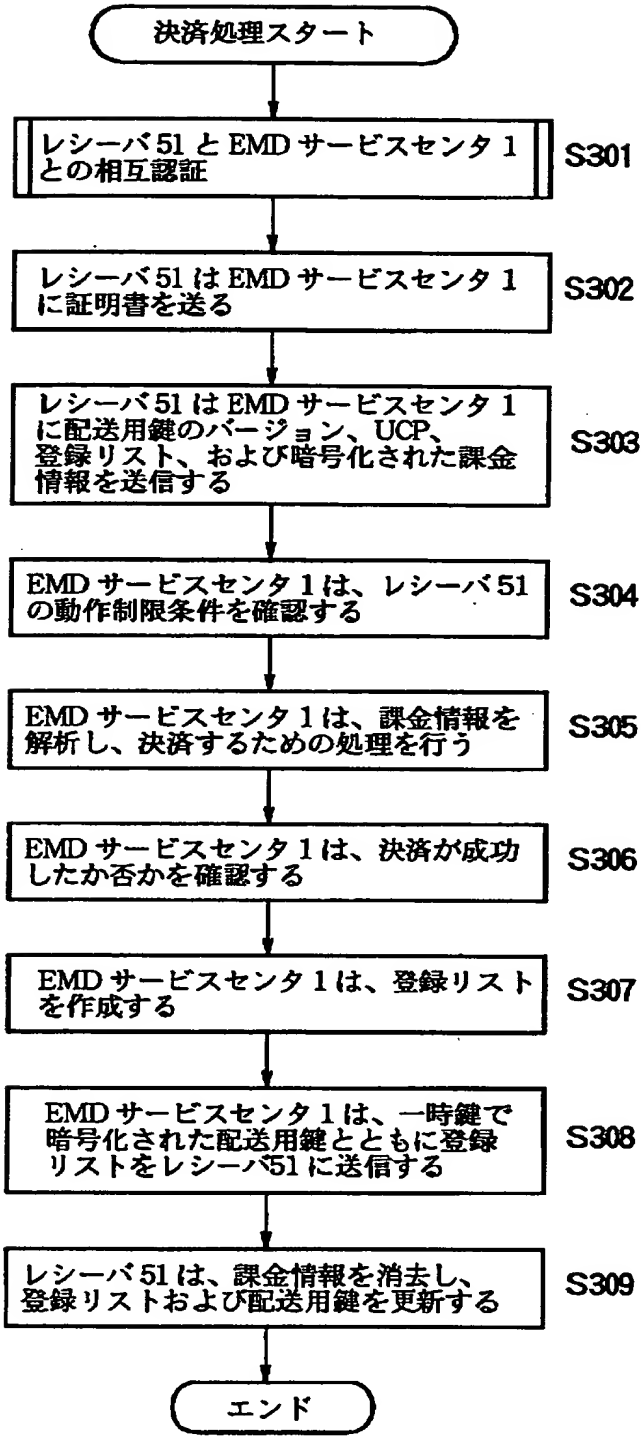
【図４６】


サービスプロバイダセキュアアコンテナの受信の処理スタート
サービスプロバイダから、セキュアコンテナを受信する
S241
サービスプロバイダから、公開鍵証明書を受信する
S242
セキュアコンテナの署名データを検証する
S243
UCPおよびPTを基に利用内容の選択
S244
UCPおよびPTを基に、課金情報およびUCSを作成する
S245
コンテンツをHDDに記録する
S246
コンテンツ鍵を配送用鍵で復号する
S247
コンテンツ鍵を保存用鍵で暗号化する
S248
外部記憶部の空きのあるブロックを検索する
S249
外部記憶部の空きのあるブロックのハッシュ値を計算する
S250
S251
算出したハッシュ値と記憶モジュールの所定の検査値が一致する?
NO
YES
S256
外部記憶部の全てのブロックを調べた?
YES
NO
S257
外部記憶部の空きのある他のブロックを検索する
コンテンツ鍵等を外部記憶部に記憶する
S252
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S253
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S254
課金情報を記憶モジュールに記憶する
S255
リターン

【図４７】


再生処理スタート
S261
ブロックのハッシュ値を計算する
S262
SAM 内の
ハッシュ値と一致する
?
NO
S277
エラー処理
YES
S263
再生可能?
NO
YES
UCS を更新する
S264
UCS を外部記憶部に記憶する
S265
検査値 Hp を算出し、記憶する
S266
SAM と伸張部で相互認証し、一時
鍵が共有される
S267
コンテンツ鍵を保存用鍵で復号する
S268
コンテンツ鍵を一時鍵で暗号化する
S269
コンテンツ鍵を伸張部に送る
S270
コンテンツ鍵を一時鍵で復号する
S271
伸張部はコンテンツを受け取る
S272
コンテンツ鍵でコンテンツを復号する
S273
コンテンツを伸張する
S274
コンテンツにウォータマークを付加する
S275
コンテンツを出力する
S276
リターン

【図４８】


決済処理スタート
レシーバ51とEMDサービスセンタ1との相互認証
S301
レシーバ51はEMDサービスセンタ1に証明書を送る
S302
レシーバ51はEMDサービスセンタ1に配送用鍵のバージョン、UCP、登録リスト、および暗号化された課金情報を送信する
S303
EMDサービスセンタ1は、レシーバ51の動作制限条件を確認する
S304
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S305
EMDサービスセンタ1は、決済が成功したか否かを確認する
S306
EMDサービスセンタ1は、登録リストを作成する
S307
EMDサービスセンタ1は、一時鍵で暗号化された配送用鍵とともに登録リストをレシーバ51に送信する
S308
レシーバ51は、課金情報を消去し、登録リストおよび配送用鍵を更新する
S309
エンド

【書類名】　　要約書

【要約】

【課題】　ユーザ情報に応じてサービスを提供できるようにする。

【解決手段】　PTA－１の「価格条件１０」の「ユーザ条件１０」には、男性のユーザであるとが示されているので、PTA－１は、男性のユーザのみが選択可能となる。PTA－２の「価格条件２０」の「ユーザ条件２０」には、女性のユーザであることが示されているので、PTA－２は、女性のユーザのみが選択可能となる。PTA－１とPTA－２の価格内容を比較すると、PTA－２の価格内容に示される額は、対応するPTA－１の価格内容に示される額の半分にされている。すなわち、女性ユーザは、男性ユーザに比べ、半額の料金でコンテンツを利用することができる。

【選択図】　　図２０

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社